Junos® OS Release 12.1X46-D10 for the Branch and High-End SRX Series and J Series

These release notes accompany Release 12.1X46-D10 of the Junos OS. They describe device documentation and known problems with the software. Junos OS runs on all Juniper Networks SRX Series Services Gateways and J Series Services Routers.

For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, which is located at https://www.juniper.net/techpubs/software/junos/.

Contents

Junos OS Release Notes for Branch SRX Series and J Series

Powered by Junos OS, Juniper Networks SRX Series Services Gateways provide robust networking and security services. SRX Series Services Gateways range from lower-end branch devices designed to secure small distributed enterprise locations to high-end devices designed to secure enterprise infrastructure, data centers, and server farms. The branch SRX Series Services Gateways include the SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

Juniper Networks J Series Services Routers running Junos OS provide stable, reliable, and efficient IP routing, WAN and LAN connectivity, and management services for small to medium-sized enterprise networks. These routers also provide network security features, including a stateful firewall with access control policies and screens to protect against attacks and intrusions, and IPsec VPNs. The J Series Services Routers include the J2320, J2350, J4350, and J6350 devices.

New and Changed Features

The following features have been added to Junos OS Release 12.1X46-D10. Following the description is the title of the manual or manuals to consult for further information.

> NOTE: For the latest updates about support and issues on Junos Pulse, see the Junos Pulse Release Notes.

Software Features

Application Layer Gateways (ALGs)

- **ALG message buffer optimization**—Starting in Junos OS Release 12.1X46-D10, the ALG message buffer optimization feature has been enhanced to reduce high memory consumption. This feature is supported on all SRX Series and J Series devices.

  A message buffer is allocated only when the packet is ready to process. The buffer is freed after the packet completes ALG handling, including modifying the payload, performing NAT, opening a pinhole for a new connection between a client and a server, and transferring data between a client and a server located on opposite sides of a Juniper Networks device.

This feature has the following enhancements:

- Unnecessary objcache buffering is avoided, resulting in low memory utilization.

- jbuf manipulation is used to simplify the message buffer logic.

- Full-fledged message buffer support for the ALG line breaker is more flexible.

- ALG Manager and ALG plug-in logic clarity are optimized.

[See alg-manager.]

- **IPv6 support for SIP ALG**—This feature is supported on all SRX Series and J Series devices.

  Starting with Junos OS Release 12.1X46-D10, IPv6 is supported on the SIP ALG along with NAT-PT mode and NAT64 address translation.

  The SIP ALG processes the IPv6 address in the same way it processes the IPv4 address for updating the payload if NAT is configured and opening pinholes for future traffic.

  NAT-PT is implemented by normal NAT from IPv6 address to IPv4 address and vice versa. The SIP ALG processes those address translations in payload just as the addresses are processed in normal NAT.

  NAT64 is a mechanism to allow IPv6 hosts to communicate with IPv4 servers. NAT64 is required to keep the IPv6 to IPv4 address mapping.

  Previously, Session Traversal Utilities for NAT (STUN) worked without the SIP ALG. This means that the SIP ALG was not involved when persistent NAT was configured.

  Starting with Junos OS Release 12.1X46-D10, STUN can coexist with the SIP ALG and SIP ALG is involved when persistent NAT is configured.

  [See SIP ALG Feature Guide for Security Devices.]

- **IPv6 support for RTSP ALG**—This feature is supported on all SRX Series and J Series devices.

  Real-Time Streaming Protocol (RTSP) is an Application Layer protocol for controlling the delivery of data with real-time properties. The RTSP ALG accesses existing media files over the network and controls the replay of the media.

  Starting with Junos OS Release 12.1X46-D10, IPv6 is supported on the RTSP ALG along with NAT-PT mode and NAT64 address translation.

  This feature enables the RTSP ALG to parse IPv6 RTSP packets, open an IPv6 pattern pinhole, and translate the Layer 7 IPv6 address according to the NAT configuration. Also, support for IPv6 RTSP transaction pass through under permission policy and IPv6 RTSP transaction pass through under NAT-PT and NAT 64 are enabled.

  [See SIP RTSP ALG Feature Guide for Security Devices.]

- **IPv6 support for PPTP ALG**—Starting with Junos OS Release 12.X46-D10, this feature is supported on all SRX Series devices.

  PPTP ALG provides an ALG for the Point-to-Point Tunneling Protocol (PPTP). The PPTP is a Layer 2 protocol that tunnels PPP data across TCP/IP networks. The PPTP

client is freely available on Windows systems and popularly applied on Linux systems; it is widely deployed for building VPNs.

To support IPv6, the PPTP ALG parses both IPv4 and IPv6 PPTP packets, performs NAT, and then opens a pinhole for the data tunnel. The flow module supports IPv6 to parse the GRE packet and use the GRE call ID as fake port information to search the session table and gate table.

- **Support for SCCP v20**—This feature is supported on all SRX Series devices.

  Starting in Junos OS Release 12.1X46-D10, the SCCP ALG supports version 20. In SCCP v20, several SCCP messages have been updated with a new format.

  [See PPTP ALG Feature Guide for Security Devices.]

AppSecure

- **Application-aware quality of service (AppQoS)**—Starting in Junos OS Release 12.1X46-D10, AppQoS is supported on all branch SRX Series devices.

  AppQoS provides a mechanism for prioritizing traffic utilizing the results of the Application Identification Engine. AppQoS provides application-level traffic control for administrators needing to ensure that business-critical applications get preferential treatment.

  AppQoS enables the network administrator to meter, mark, and honor traffic priority based on application policies. It provides application-aware DSCP marking by implementing Layer 7 application-based DSCP rewriters. To apply different loss priority levels to different traffic groups, Layer 2-based to Layer 4-based honoring has been expanded to Layer 7. AppQoS accomplishes application-aware rate limiting by setting the bandwidth limit and burst size limit for different applications.

  [See Understanding Application QoS (AppQoS).]

Dynamic Host Configuration Protocol (DHCP)

- **DHCP relay**—Starting in Junos OS Release 12.1X46-D10, the existing DHCP relay feature on all branch SRX Series devices has been enhanced to include chassis cluster support.

  [See Understanding DHCP Relay Agent Operation.]

Flow and Processing

- **Enhanced IPv6 support for the screen feature**—This feature is supported on all branch SRX Series and J Series devices.

  IPv6 support is extended for the following screen features:

  - IPv6 extension header checking and filtering

  - IPv6 packet header checking and filtering

  - ICMPv6 checking and filtering

  New statements and commands allow you to configure these enhancements using security zones similar to previous screen configurations. You can enable, disable, and

update screens to drop packets, create logs, and provide increased statistics for IPv6 traffic.

> **NOTE:** By default, IPv6 packets bypass the screen feature.

[See Understanding IPv6 Support for Screens.]

- **Enhanced IPv6 support for flow**—This feature is supported on all branch SRX Series and J Series devices.

  IPv6 support is extended for checking and filtering IPv6 extension headers (in accordance with RFC 2460) and IPv6 link-local addresses (in accordance with RFC 4291) in a flow. Nonconforming IPv6 packets will be discarded.

- **Enhancements to flow trace options**—This feature is supported on all branch SRX Series and J Series devices.

  Starting in Junos OS Release 12.1X46-D10, flow trace granularity has been enhanced to filter logs effectively. As a result you can access relevant trace messages easily and avoid large traces that slow down your system. You can set the level of message you want displayed by using the new **trace-level** statement at the **[edit security flow traceoptions]** hierarchy level. You can use new flags to trace additional operations such as fragmentation, high availability, multicast, session, tunnel, and route.

  [See traceoptions (Security Flow).]

- **Monitoring flow sessions**—This feature is supported on all branch SRX Series and J Series devices.

  Beginning with Junos OS Release 12.1X46-D10, you can monitor flow using filters that match different criteria (such as source and destination addresses). New operational mode commands **monitor security flow filter** and **monitor security flow file** have been added. These commands allow you to debug without having to commit or modify your running configuration. Previously, you were required to commit the configuration to turn on trace options, which could possibly change the state of your device.

  [See Monitoring Security Flow Sessions Overview.]

Intrusion Detection and Prevention (IDP)

- **IDP IPv6 inspection**—Starting in Junos OS Release 12.1X46-D10, IDP supports IPv6 inspection on the SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650. IPv6 builds upon the functionality of IPv4, providing improvements to addressing, configuration and maintenance, and security.

  This feature supports:

  - IPv6 traffic inspection

  - Attack detection inspection in protocol decoders that support IPv6

  - IDP signature database

- IDP logging

- Application identification results

Use the **show security flow session idp family** command with the **inet** or **inet6** option to view IPv4 or IPv6 statistics.

[See IDP Monitoring and Troubleshooting Guide for Security Devices.]

- **IDP security packet capture**—Starting in Junos OS Release 12.1X46-D10, this feature is supported on the SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650.

Viewing packets that precede and follow an attack helps you determine the purpose and extent of an attempted attack, whether an attack was successful, and if any network damage was caused. Packet analysis also aids in defining attack signatures to minimize false positives.

Use the **show security idp counters packet-log** command to display details about the progress, success, and failure of packet capture activity.

You can specify pre-attack, post-attack, and post-attack timeout values. The pre-attack and post-attack default values are 1, and the default post-attack timeout value is 5.

> **NOTE:** Support for packet capture is available only once on each session.

[See Understanding Security Packet Capture.]

IPsec VPN

- **Support for IPv6 address encapsulation in route-based one-to-one site-to-site VPN tunnels**—This feature is supported on all SRX Series devices.

In tunnel mode, IPsec encapsulates the original IP datagram—including the original IP header—within a second IP datagram. The outer IP header contains the IP address of the gateway, while the inner header contains the ultimate source and destination IP addresses. The outer and inner IP headers can have a protocol field of IPv4 or IPv6. As of Junos OS Release 12.1X46-D10, the following tunnel modes are supported on SRX Series devices:

- IPv4-in-IPv4 tunnels encapsulate IPv4 packets inside IPv4 packets.

- IPv6-in-IPv6 tunnels encapsulate IPv6 packets inside IPv6 packets.

- IPv6-in-IPv4 tunnels encapsulate IPv6 packets inside IPv4 packets.

- IPv4-in-IPv6 tunnels encapsulate IPv4 packets inside IPv6 packets.

There are no new CLI configuration statements for this feature.

IPv4 and IPv6 traffic can be routed into a single IPv4 or IPv6 tunnel; the st0 interface bound to the tunnel must be configured for both family inet and family inet6. Dual stack tunnels—parallel IPv4 and IPv6 tunnels over a single physical external interface to different VPN peers—are also supported.

[See VPN Feature Support for IPv6 Addresses.]

- **Dead peer detection (DPD) enhancements**—This feature is supported on all SRX Series devices.

  Network devices use the DPD protocol to verify the existence and availability of other peer devices. The default DPD mode **optimized** sends probes if there is no incoming IKE or IPsec traffic from the peer within a configured interval after outgoing packets are sent to the peer. The **always-send** option sends DPD probes at configured intervals regardless of traffic activity between peers. A new configuration option **probe-idle-tunnel** at the [**edit security ike gateway dead-peer-detection**] hierarchy level sends DPD probes when there is no incoming or outgoing IKE or IPsec traffic between peers.

  > **NOTE:** We recommend that you configure **probe-idle-tunnel** instead of **always-send**.

  For all DPD modes, Phase 1 and Phase 2 security associations are cleared if a specified number of probes are sent with no response from the peer.

  [See Understanding Dead Peer Detection.]

- **Multiple traffic selectors on a route-based VPN**—This feature is supported on all branch SRX Series devices.

  A traffic selector (also known as a proxy ID in IKEv1) is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. With this feature, you can define multiple traffic selectors within a specific route-based VPN, resulting in a unique SA for each traffic selector configured. Only traffic that conforms to a traffic selector is permitted through the associated IPsec SA.

  To configure a traffic selector, use the **traffic-selector** configuration statement at the [**edit security ipsec vpn** *vpn-name*] hierarchy level. The traffic selector pair is defined with the mandatory **local-ip** *ip-address* and **remote-ip** *ip-address* statements. The CLI operational command **show security ipsec security-association traffic-selector** *traffic-selector* displays SA information for the specified traffic selector.

  [See Understanding Traffic Selectors in Route-Based VPNs.]

- **IKEv2 configuration payload support with RADIUS**—This feature is supported on all SRX Series devices.

  Configuration payload is an Internet Key Exchange (IKE) version 2 feature used to propagate provisioning information from an IKE responder to the IKE initiator. Starting with Junos OS Release 12.1X46-D10, IKEv2 configuration payload is supported with route-based VPNs only. The following attribute types, defined in RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)*, can be returned to the IKE initiator by the IKE responder:

  - INTERNAL_IP4_ADDRESS

  - INTERNAL_IP4_NETMASK

  - INTERNAL_IP4_DNS

For the IKE responder to provide the initiator with provisioning information, it must acquire the information from a specified source such as a RADIUS server. Provisioning information can also be returned from a DHCP server through a RADIUS server. On the RADIUS server, the user information should not include an authentication password. As in previous Junos OS releases for the SRX Series, the RADIUS server profile is bound to the IKE gateway using the xauth access-profile *profile-name* configuration at the [edit security ike gateway *gateway-name*] hierarchy level.

This feature is supported only for point-to-multipoint secure tunnel (st0) interfaces. For point-to-multipoint interfaces, the interfaces must be numbered and the addresses in the configuration payload INTERNAL_IP4_ADDRESS attribute type must be within the subnetwork range of the associated point-to-multipoint interface.

> NOTE: IKEv2 on SRX Series devices does not support policy-based VPNs or VPN monitoring.

[See Understanding Internet Key Exchange Version 2.]

- **IKEv2 with NAT-T and dynamic endpoint VPN**—This feature is supported on all SRX Series devices.

  Starting with Junos OS 12.1X46-D10, both IKEv2 initiators and responders in a route-based VPN can be behind NAT devices. The IKEv2 NAT-T feature supports IPsec traffic that crosses NAT devices. Static NAT and dynamic NAT are supported. In static NAT, there is a one-to-one relationship between the private and the public addresses. In dynamic NAT, there is a many-to-one or many-to-many relationship between the private and public addresses.

  Dynamic endpoint (DEP) VPN is a Junos OS feature that covers IKEv2 initiator and responder perspectives. From the initiator's perspective, DEP VPN covers the situation where the IKE external interface address is not fixed and is therefore not known by the responder. This situation can occur when the peer's address is dynamically assigned by an ISP or when the peer's connection crosses a NAT device that allocates addresses from a dynamic address pool. From the responder's perspective, DEP VPN describes either a finite number of VPNs that are created for a number of VPN peers in a many-to-many scenario or a shared VPN in a many-to-one scenario.

  Starting with Junos OS 12.1X46-D10, the default value for the **nat-keepalive** option configured at the [edit security ike gateway *gateway-name*] hierarchy level has been changed from 5 seconds to 20 seconds.

  [See Understanding NAT-T.]

IP Spoofing

- **IP spoofing in transparent mode**—Starting in Junos OS Release 12.1X46-D10, this feature is supported on all branch SRX Series devices.

  The IP spoofing feature has been enhanced to include Layer 2 transparent mode support. IP spoofing is most frequently used in denial-of-service attacks. In an IP spoofing attack, the attacker gains access to a restricted area of the network and inserts a false source address in the packet header to make the packet appear to come from a trusted source. When SRX Series devices are operating in transparent mode, the IP spoof-checking mechanism makes use of address book entries.

  > NOTE:
  > - IP spoofing in Layer 2 transparent mode does not support DNS and wildcard addresses.
  >
  > - IP spoofing in Layer 2 transparent mode is not supported on IPv6, because branch SRX Series devices do not support IPv6 in Layer 2 transparent mode.

  [See Understanding IP Spoofing in Layer 2 Transparent Mode.]

J-Web

- **Management support for NAT options**—Starting in Junos OS Release 12.1X46-D10, support is provided to monitor the following NAT options on all SRX Series devices:

  - Utilization for all source pools

  - Successful, failed, and current sessions for source pools, source rules, destination rules, and static rules

  - Source addresses and source ports for static rules

  - Source ports for source rules

- Support is provided to configure the following NAT options on all SRX Series devices:

  - Source address and port as match criteria for static rules

  - Source port as match criteria for source rules

  - Upper and lower thresholds at which an SNMP trap is triggered for source rules and pools, destination rules, and static rules

- **User firewall J-Web support**

  - **Source identity-based firewall policy**—Starting in Junos OS Release 12.1X46-D10, this feature is supported on the existing Firewall Policies Configuration and Monitoring Policies pages on all branch SRX Series devices. This feature allows you to configure and monitor source identities in a firewall policy.

  - **New J-Web pages for user firewall**—Starting in Junos OS Release 12.1X46-D10, new user firewall pages are supported on all branch SRX Series devices.

The following webpages have been added to the J-Web user interface:

- **Authentication Priority Configuration Page**—You can either disable an optional authentication source or reassign a unique priority to it.

- **Local Authentication Configuration Page and Local Authentication Monitoring Page**—You can configure and monitor local Firewall authentication.

- **UAC Settings Configuration Page and UAC Authentication Monitoring Page**—You can configure UAC and monitor UAC authentication.

- **Allow adding a new policy and moving an existing policy to an arbitrary location**

  - **Firewall Policies Configuration Page Options**—Starting in Junos OS Release 12.1X46-D10, several new options on the Firewall Policies Configuration page are supported on all branch SRX Series devices. The Add menu includes Add before and Add after options that allow you to add a new policy before or after a selected policy. On the Move menu, there is a new Move to option that allows you to specify a target location. You can also drag and drop a policy to the target location.

  - **Checking Policies Monitoring Page**—Starting in Junos OS Release 12.1X46-D10, the Move to option on the Checking Policies Monitoring page is supported on all branch SRX Series devices.

Management Information Bases (MIBs)

- **SNMP aggregation for policy MIBs**—Starting in Junos OS Release 12.1X46-D10, this feature is supported on all SRX Series devices.

  A set of systemwide policy statistics such as policy-allowed packets, bytes and rates, policy-dropped packets, bytes and rates, policy flows allowed, and rate statistics have been added in the enterprise-specific policy MIB JUNIPER-JS-POLICY-MIB. You can obtain the policy statistics by using the SNMP agent or the CLI operational mode commands. Use the following CLI commands to set, clear, and display the systemwide policy statistics:

  - **set security policies policy-stats system-wide <disable | enable>**—Configures systemwide policy statistics. Disabled by default.

  - **clear security policies statistics**—Clears the systemwide policy statistics.

  - **show snmp mib walk jnxJsPolicySystemStats**—Displays both IPv4 and IPv6 statistics.

  - **show snmp mib walk jnxJsPolicySystemStatsIPv4**—Displays only IPv4 statistics.

[See Policy Objects MIB.]

Virtual Private Networks (VPNs)

- **Enhanced X2 interface monitoring**—This feature is supported on all SRX Series devices.

  In an LTE mobile network, X2 interfaces are used to connect Evolved Node Bs (eNodeBs) for signal handover, monitoring, and radio coverage. SRX Series devices connect these eNodeBs using IPsec tunnels.

  This feature enables you to monitor traffic between eNodeBs by snooping into the clear text traffic as it flows from one IPsec tunnel to another. Use the **monitor-filter** statement at the **[edit security forwarding-options]** hierarchy level to duplicate clear text packets and send them to the physical interface. You can then use Ethereal or other packet analyzers to verify or collect the X2 traffic.

  [See Understanding X2 Traffic Monitoring]

Web Authentication

- **Web-redirect firewall authentication**—Starting in Junos OS Release 12.1X46-D10, Web authentication redirect enhancement is provided on all SRX Series devices.

  With this feature, when you attempt to initiate a connection across the firewall, after successful authentication the browser launches your original destination URL without you needing to retype the URL.

  The following message is displayed:

  ```
  Redirecting to the original url, please wait
  ```

  [See Firewall User Authentication Overview]

Related Documentation
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 24
- Known Issues on page 53
- Resolved Issues on page 57
- Documentation Updates on page 63
- Migration, Upgrade, and Downgrade Instructions on page 70

Changes in Behavior and Syntax

The following current system behavior, configuration statement usage, and operational mode command usage might not yet be documented in the Junos OS documentation:

Application Firewall

- Prior to Junos OS Release 11.4R6, when a rule specifies **dynamic-application junos:HTTP** without specifying any other nested application, the rule matches all HTTP traffic whether the traffic contains a nested application or not.

In Junos OS Release 11.4R6 and later, that functionality has changed. When a rule specifies **dynamic-application junos:HTTP**, only HTTP traffic with no nested members is matched.

Consider the following application firewall ruleset:

```
rule-sets http-ruleset {
    rule rule1 {
        match {
            dynamic-application [junos:HTTP];
        }
        then {
            deny;
        }
    }
    default-rule {
        permit;
    }
}
```

Prior to Junos OS Release 11.4R6, the sample rules would be applied to traffic as shown in the following list:

- HTTP traffic with or without nested applications would be denied by rule1.

  HTTP traffic with a nested application, such as junos:FACEBOOK or junos:TWITTER, would be denied by rule1.

- All other traffic would be permitted by the default rule.

In Junos OS Release 11.4R6 and later, the dynamic application junos:HTTP matches only the HTTP traffic that contains no recognizable nested application. The sample rules would now be applied differently:

- Only the HTTP traffic with no nested application would be denied by rule1.

  HTTP traffic with a nested application, such as junos:FACEBOOK or junos:TWITTER, would no longer match rule1.

- All other traffic would be permitted by the default rule.

  HTTP traffic with a nested application, such as junos:FACEBOOK or junos:TWITTER, would be permitted by the default rule.

- In Junos OS Release 12.1X46-D10 and earlier, if a nested application is not configured in any rule, then the nested application would match the default rule and take action specified in the default rule.

  Starting in Junos OS Release 12.1X46-D10, the functionality has changed. If a nested application matches the default rule, then the application firewall uses the application type to match the rule and takes action specified in the rule. Use the **set security application-firewall nested-application dynamic-lookup enable** command to control the behavior of the nested application, so that both the application and the nested application are consistent.

  The default behavior of nested application before Junos OS Release 12.1X46-D10:

- Application firewall matches with the specific rule, if the nested application is configured explicitly in a rule.

- Application firewall matches with the default rule, if the nested application is not configured explicitly in a rule.

- Records the statistics of the application firewall in the matched rule.

The new behavior of nested application in Junos OS Release 12.1X46-D10:

- Application firewall matches with an application rule during application firewall policy lookup, if there is no explicit rule for the nested application.

- Application firewall matches with a specific rule, if the nested application is configured explicitly in a rule.

- Records the statistics of the application firewall in the matched rule.

Command-Line Interface (CLI)

New or Changed CLI

- Prior to Junos OS Release 12.1X46-D10, when you configured the DNS proxy server using the **set system services dns dns-proxy view** *view-name* **domain** *domain-name* **forwarder** CLI statement, if the IP address specified in the forwarder option was not available, the DNS query was forwarded to the default DNS servers (DNS servers provided by the ISP). The device acquired the public IP addresses from the default DNS servers.

  Starting in Junos OS Release 12.1X46-D10, the **forward-only** option is added to the **set system services dns dns-proxy view** *view-name* **domain** *domain-name* **forward-only** CLI statement.

  You can use the **forward-only** option to prevent the device from acquiring the public IP addresses from the DNS servers (by terminating the DNS query) in cases when the specified IP address is unreachable.

- On all branch SRX Series and J Series devices, the following commands are now supported:

CLI Command	Description
show pppoe interfaces	List all PPPoE sessions.
request pppoe connect	Connect to all sessions that are down.
request pppoe connect *pppoe interface name*	Connect only to the specified session.
request pppoe disconnect	Disconnect all sessions that are up.
request pppoe disconnect *session id* or *pppoe interface name*	Disconnect only the specified session, identified by either a session ID or a PPPoE interface name.

- On all J Series devices, a new CLI **request system (halt | power-off | reboot) power-off fpc** command has been introduced to bring Flexible PIC Concentrators (FPCs) offline before Routing Engines are shut down. This command prevents the short network outage because of the Layer 2 loop.

CLI Command	Description
request system halt power-off fpc	Bring FPC offline and then halt the system.
request system power-off power-off fpc	Bring FPC offline and then power off the system.
request system reboot power-off fpc	Bring FPC offline and then reboot the system.

Deprecated Items for Security Hierarchy

- lists deprecated items (such as CLI statements, commands, options, and interfaces).

CLI statements and commands are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration. We strongly recommend that you phase out deprecated items and replace them with supported alternatives.

Table 1: Items Deprecated in Release 12.1

Deprecated Item	Replacement	Hierarchy Level or Command Syntax	Additional Information
download-timeout	–	download-timeout timeout	On all branch SRX Series devices, the **download-timeout** command is deprecated. If the configuration is present, then that configuration will be ignored. The IDP process internally triggers the security package to install when an automatic download is completed. There is no need to configure any download timeout.
node	–	request security idp security-package download	On all branch SRX Series devices operating in a chassis cluster, the **request security idp security-package download** command with the **node** option is not supported: **request security idp security-package download node primary** **request security idp security-package download node local** **request security idp security-package download node all**

Compatibility

- **Version compatibility for Junos SDK**—Beginning with Junos OS Release 12.1X44-D10, Junos OS applications will install on the Junos OS only if the application is built with the same release as the Junos OS release on which the application is being installed.

  For example, an application built with Junos OS Release 12.1R2 will only install on Junos OS Release 12.1R2 and will not install on Junos OS Release 12.1R1 or Junos OS Release 12.1R3.

Flow and Processing

- The minimum value you can configure for TCP session initialization is 4 seconds. The default value is 20 seconds; if required you can set the TCP session initialization value to less than 20 seconds.

- On all branch SRX Series devices, the default value of type of service (ToS) for IKE packets has been changed from 0x00 to 0xc0.

- On all branch SRX Series and J Series devices, you can configure the TCP session timeout in a half-closed state by using the **apply-to-half-close-state** statement at the **[edit security flow tcp-session time-wait-state]** hierarchy level. This enables the system to apply the configured session timeout on receiving only one FIN packet (either client-to-server or server-to-client). When this statement is not configured, the default behavior takes effect, which is to apply the configured session timeout on receiving both the FIN packets. The default TCP session timeout remains 150 seconds. [See *apply-to-half-close-state*.]

Hardware

- On SRX550 devices, the mini-USB console cable provides a "break" message to the Windows application whenever the console cable is unplugged and re-plugged. If you have configured "debugger-on-break", the system goes to the **db>** prompt because the system receives a break character. This behavior is specific to the mini-USB console.

Interfaces and Routing

- On SRX240 and SRX650 devices, for the Layer 2 LAG interface, the hash algorithm for load balancing is now based on source IP address and destination IP address instead of source MAC address and destination MAC address.

Intrusion Detection and Prevention (IDP)

- By default, values for IDP reassembler packet memory and application identification packet memory used by IDP are established as percentages of all memory. In most cases, these default values are adequate.

  - If a deployment exhibits an excessive number of dropped TCP packets or retransmissions resulting in high IDP reassembly memory usage, use the following option:

    The **max-packet-mem-ratio** option to reset the percentage of available IDP memory for IDP reassembly packet memory. Acceptable values are between 5 and 40 percent.

```
set security idp sensor-configuration re-assembler max-packet-mem-ratio
    percentage-value
```

> NOTE: The **max-packet-mem** option has been deprecated and replaced by the new **max-packet-mem-ratio** option.

- If a deployment exhibits an excessive number of ignored IDP sessions due to reassembler and application identification memory allocation failures, use the following options:

  - The **max-packet-memory-ratio** option sets application identification packet memory limit as a percentage of available IDP memory. This memory is only used by IDP in cases where application identification delays identifying an application. Acceptable values are between 5 and 40 percent.

    ```
    set security idp sensor-configuration application-identification
        max-packet-memory-ratio percentage-value
    ```

  - The **max-reass-packet-memory-ratio** option sets the reassembly packet memory limit for application identification as a percentage of available IDP memory. Acceptable values are between 5 and 40 percent.

    ```
    set security idp sensor-configuration application-identification
        max-reass-packet-memory-ratio percentage-value
    ```

    > NOTE: The **max-packet-memory** option has been deprecated and replaced by the new **max-packet-memory-ratio** and **max-reass-packet-memory-ratio** options.

J-Web

- On all branch SRX Series and J Series devices, the username field does not accept HTML tags or the "<" and ">" characters. The following error message appears:

  ```
  A username cannot include certain characters, including < and >
  ```

- On all branch SRX Series devices, on the Monitoring Policies page, the Deactivate and Move functions on the toolbar and the Count and Log action columns in the output table are not supported and will no longer be available.

- On all branch SRX Series devices, on the Checking Policies page, the Delete and Deactivate buttons are not supported and will no longer be available.

Logical Systems

- In Junos OS releases earlier than Junos OS Release 12.1X46-D10, when a logical tunnel interface with an IPv4 address and an Ethernet encapsulation type is configured, a configuration check is performed to ensure that the address is not identical to its peer logical tunnel interface address and that both addresses are on the same subnet. However, when a logical tunnel interface with an IPv6 address and an Ethernet encapsulation type is configured, no such configuration check is performed.

  Starting in Junos OS Release 12.1X46-D10, a check is performed for IPv6 configurations. However, this change can cause existing IPv6 configurations to fail.

Simple Network Management Protocol (SNMP)

- On all branch SRX Series and J Series devices, the screen SNMP trap **jnxJsScreenCfgChange** will not be sent during reboot.

System Logs

On all branch SRX Series devices, the following system log messages have been updated to include the **certificate ID**:

- PKID_PV_KEYPAIR_DEL

  Existing message: **Key-Pair deletion failed**

  New message: **Key-Pair deletion failed for <cert-id>**

- PKID_PV_CERT_DEL

  Existing message: **Certificate deletion has occurred**

  New message: **Certificate deletion has occurred for <cert-id>**

- PKID_PV_CERT_LOAD

  Existing message: **Certificate has been successfully loaded**

  New message: **Certificate <cert-id> has been successfully loaded**

- PKID_PV_KEYPAIR_GEN

  Existing message: **Key-Pair has been generated**

  New message: **Key-Pair has been generated for <cert-id>**

Virtual Private Networks (VPNs)

- On all branch SRX Series devices, for path MTU calculations, the IPsec authentication data length is fixed at 16 bytes. However, the authentication data length for packets going through the IPsec tunnel is in accordance with the authentication algorithm negotiated for that tunnel.

  The authentication data lengths for the different algorithms are:

  - hmac-md5-96 (12 bytes)

- hmac-sha-256-128 (16 bytes)

- hmac-sha1-96 (12 bytes)

- For each VPN tunnel, both ESP and AH tunnel sessions are installed on SPUs and the control plane. In previous Junos OS releases, two tunnel sessions of the same protocol (ESP or AH) were installed for each VPN tunnel. For branch SRX Series devices, tunnel sessions are updated with the negotiated protocol after negotiation is completed. For high-end SRX Series devices, tunnel sessions on anchor SPUs are updated with the negotiated protocol while non-anchor SPUs retain ESP and AH tunnel sessions.

  The ESP and AH tunnel sessions are displayed in the outputs for the **show security flow session** and **show security flow cp-session** operational mode commands.

- As of Junos OS Release 11.4, checks are performed to validate the IKE ID received from the VPN peer device. By default, SRX Series and J Series devices validate the IKE ID received from the peer with the IP address configured for the IKE gateway. In certain network setups, the IKE ID received from the peer (which can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address) does not match the IKE gateway configured on the SRX Series or J Series device. This can lead to a Phase 1 validation failure.

  To modify the configuration of the SRX Series or J Series device or the peer device for the IKE ID that is used:

  1. On the SRX Series or J Series device, configure the **remote-identity** statement at the [**edit security ike gateway** *gateway-name*] hierarchy level to match the IKE ID that is received from the peer. Values can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address.

     NOTE: If you do not configure remote-identity, the device uses the IPv4 or IPv6 address that corresponds to the remote peer by default.

  2. On the peer device, ensure that the IKE ID is the same as the **remote-identity** configured on the SRX Series or J Series device. If the peer device is an SRX Series or J Series device, configure the **local-identity** statement at the [**edit security ike gateway** *gateway-name*] hierarchy level. Values can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address.

- The subject fields of a digital certificate can include Domain Component (DC), Common Name (CN), Organization Unit (OU), Organization (O), Location (L), State (ST), and Country (C).

  In earlier releases, the **show security pki ca-certificate** and **show security pki local-certificate** CLI operational commands displayed only a single entry for each subject field, even if the certificate contained multiple entries for a field. For example, a certificate with two OU fields such as "OU=Shipping Department, OU=Priority Mail" displayed with only the first entry "OU=Shipping Department." The **show security pki ca-certificate** and **show security pki local-certificate** CLI commands now display the entire contents of the subject field, including multiple field entries.

The commands also display a new subject string output field that shows the contents of the subject field as it appears in the certificate.

- When a remote user launches newly installed client software, the link to close the Web browser window does not appear in the VPN client launch page. The user must close the browser window by clicking the browser's close button.

Related Documentation

Known Behavior

Application Layer Gateways (ALGs)

- The maximum size of the jbuf is 9 Kb. If the message buffer size is more than 9 Kb, the entire message cannot be transferred to the ALG packet handler. This causes subsequent packets in the session to bypass ALG handling, resulting in a transaction failure.

The limitations for SCCP ALGs are as follows:

- The SCCP is a Cisco proprietary protocol. So, any changes to the protocol by Cisco cause the SCCP ALG implementation to break. However, workarounds are provided to bypass strict decoding and allow any protocol changes to be handled gracefully.

- The SCCP ALG validates protocol data units (PDUs) with message IDs in the ranges [0x0 - 0x12], [0x20 - 0x49], and [0x81 - 0x14A]. By default, all other message IDs are treated as unknown messages and are dropped by the SCCP ALG.

- Any changes to the policies will drop the sessions and impact already established SCCP calls.

- The SCCP ALG opens pinholes that are collapsed during traffic or media inactivity. This means that during a temporary loss of connectivity, media sessions are not reestablished.

- CallManager (CM) version 6.x and later does not support TCP probe packets in chassis cluster mode. As a result, the existing SCCP sessions will break when there is a failover. You can still create new SCCP sessions during failover.

The PPTP ALG with IPv6 support has the following limitation:

- Because PPP packets are compressed with Microsoft Point-to-Point Encryption (MPPE) protocol after the tunnel is set up, translation of the IP header in the PPP package cannot be handled; therefore, to make sure PPTP connection works well, the PPTP client must be able to work in dual stack mode. So that an IPv6 PPTP client can accept an IPv4 address for PPP tunnel interface, by which it can communicate with the IPv4 PPTP server without IP address translation for PPP packets.

The RTSP ALG with IPv6 support has the following limitations:

- Real-Time Streaming Protocol (RTSP) is an Application Layer protocol for controlling the delivery of data with real-time properties. The RTSP ALG supports a peer client, and the server transmits real-time media; it does not support third-party endpoints involved in the transaction.

- In case of destination NAT or NAT64 for IP address translation, if the RTSP message (including the Session Description Protocol (SDP) application content) length exceeds 2500 bytes, then the RTSP ALG processes only the first 2500 bytes of the message and ignores the rest of the message. In this scenario, the IP address in the RTSP message is not translated if the IP address does not appear in the first 2500 bytes.

The SIP ALG with IPv6 support has the following limitation:

- When NAT64 with persistent NAT is implemented, the SIP ALG adds the NAT translation to the persistent NAT binding table if NAT is configured on the Address of Record (AOR). Because persistent NAT cannot duplicate the address configured, coexistence of NAT66 and NAT64 configured on the same address is not supported.

  Only one binding is created for the same source IP address.

AppSecure

- J-Web pages for AppSecure are preliminary.

- Custom application signatures and custom nested application signatures are not currently supported by J-Web.

- When ALG is enabled, application identification includes the ALG result to identify the application of the control sessions. Application firewall permits ALG data sessions whenever control sessions are permitted. If the control session is denied, there will be no data sessions. When ALG is disabled, application identification relies on its signatures to identify the application of the control and data sessions. If a signature match is not found, the application is considered unknown. Application firewall handles applications based on the application identification result.

AX411 Access Points

- On SRX210, SRX240, and SRX650 devices, you can configure and manage a maximum of four access points.

- On all branch SRX Series devices, managing AX411 WLAN Access Points through a Layer 3 ae interface is not supported.

Chassis Cluster

- SRX100, SRX210, SRX240, and SRX650 devices have the following chassis cluster limitations:

  - VRRP is not supported.

  - Unified ISSU is not supported.

  - The 3G dialer interface is not supported.

  - On SRX Series device failover, access points on the Layer 2 switch reboot and all wireless clients lose connectivity for 4 to 6 minutes.

  - VDSL Mini-PIMs are not supported in chassis cluster.

  - Queuing on the ae interface is not supported.

  - Group VPN is not supported.

  - Sampling features such as flow monitoring, packet capture, and port mirror on the reth interfaces are not supported.

  - On SRX100 and SRX110 devices, switching is not supported in chassis cluster mode.

  - The Chassis Cluster MIB is not supported.

  - Any packet-based services such as MPLS and CLNS are not supported.

  - On the lsq-0/0/0 interface, Link services MLPPP, MLFR, and CRTP are not supported.

  - On the lt-0/0/0 interface, CoS for RPM is not supported.

- Packet-based forwarding for MPLS and ISO protocol families is not supported.

- The factory default configuration for SRX100 devices automatically enables Layer 2 Ethernet switching. Layer 2 Ethernet switching is not supported in chassis cluster mode for SRX100 devices. If you use the factory default configuration, you must delete Ethernet switching before you enable chassis clustering.

- On all J Series devices, a Fast Ethernet port from a 4-port Ethernet PIM cannot be used as a fabric link port in a chassis cluster.

- On all branch SRX Series devices, reth interfaces and the lo0 interface are supported for IKE external interface configuration in IPsec VPN. Other interface types can be configured, but IPsec VPN might not work.

- On all J Series devices, the ISDN feature on chassis cluster is not supported.

Command-Line Interface (CLI)

- On all branch SRX Series and J Series devices, the **clear services flow** command is not supported.

- On all J Series devices, RADIUS accounting is not supported.

- On SRX210 and SRX240 devices, J-Web crashes if more than nine users log in to the device by using the CLI. The number of users allowed to access the device is limited as follows:

    - For SRX210 devices: four CLI users and three J-Web users

    - For SRX240 devices: six CLI users and five J-Web users

- On J6350 devices, there is a difference in the power ratings provided by user documentation (*J Series Services Routers Hardware Guide* and PIM, uPIM, and ePIM Power and Thermal Calculator) and the power ratings displayed by CLI (by a unit of 1). The CLI display rounds off the value to a lower integer, and the ratings provided in user documentation round off the value to the higher integer. As a workaround, follow the user documentation for accurate ratings.

- On all branch SRX Series devices, the tunnel-queuing option is not supported in chassis cluster mode.

Connectivity Fault Management (CFM)

- CFM is not supported on the following interfaces:

    - 8-Port Gigabit Ethernet SFP XPIM

    - 2-Port 10-Gigabit Ethernet XPIM

    - 1-Port SFP Mini-PIM

- CFM is supported only on interfaces with the Ethernet switching family.

Dynamic Host Configuration Protocol (DHCP)

- On all branch SRX Series devices, DHCP relay is unable to update the binding status based on DHCP_RENEW and DHCP_RELEASE messages.

- On all branch SRX Series and J Series devices, DHCPv6 client authentication is not supported.

- On all branch SRX Series and J Series devices, DHCP is not supported in a chassis cluster.

- On all branch SRX Series devices, DHCPv6 client does not support:

    - Temporary addresses

    - Reconfigure messages

    - Multiple identity association for nontemporary addresses (IA_NA)

    - Multiple prefixes in a single identity association for prefix delegation (IA_PD)

    - Multiple prefixes in a single router advertisement

Flow and Processing

- On all branch SRX Series and J Series devices, a mismatch between the Firewall Counter Packet and Byte Statistics values, and between the Interface Packet and Byte Statistics values, might occur when the rate of traffic increases above certain rates of traffic.

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, due to a limit on the number of large packet buffers, Routing Engine based sampling might run out of buffers for packet sizes greater than or equal to 1500 bytes and hence those packets will not be sampled. The Routing Engine could run out of buffers when the rate of the traffic stream is high.

- On SRX100 and SRX240 devices, the data file transfer rate for more than 20 Mbps is reduced by 60 percent with the introduction of Junos Pulse 1.0 client as compared to the Acadia client that was used before Junos OS Release 11.1.

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default authentication table capacity is 10,000; the administrator can increase the capacity to a maximum of 15,000.

- On all branch SRX Series and J Series devices, when devices are operating in flow mode, the Routing Engine side cannot detect the path MTU of an IPv6 multicast address (with a large size packet).

- On all branch SRX Series devices, you cannot configure route policies and route patterns in the same dial plan.

- On all J Series devices, even when forwarding options are set to drop packets for the ISO protocol family, the device forms ES-IS adjacencies and transmits packets because ES-IS packets are Layer 2 terminating packets.

- On all branch SRX Series and J Series devices, high CPU utilization triggered for reasons such as CPU intensive commands and SNMP walks causes the BFD protocol to flap while processing large BGP updates.

- On SRX210, SRX240, and J Series devices, broadcast TFTP is not supported when flow is enabled on the device.

- On SRX210, SRX240, and SRX650 devices, the maximum number of concurrent sessions for SSH, Telnet, and Web is as follows:

Sessions	SRX210	SRX240	SRX650
SSH	3	5	5
Telnet	3	5	5
Web	3	5	5

NOTE: These defaults are provided for performance reasons.

- On SRX210 and SRX240 devices, for optimized efficiency, we recommend that you limit use of CLI and J-Web to the numbers of sessions listed in the following table:

Device	CLI	J-Web	Console
SRX210	3	3	1
SRX240	5	5	1

- On SRX100 devices, Layer 3 control protocols (OSPF, using multicast destination MAC address) on the VLAN Layer 3 interface work only with access switch ports.

Interfaces and Routing

- On SRX100, SRX110, SRX210, and SRX220 devices, you cannot configure the same VRRP group ID on different interfaces of a single device.

- On all J Series devices, the flow monitoring version 9 has the following limitations:

  - Routing Engine based flow monitoring V5 or V8 mode is mutually exclusive with inline flow monitoring V9.

  - Flow aggregation for V9 export is not supported.

  - Only UDP over IPv4 or IPv6 protocol can be used as the transport protocol.

  - Only the standard IPv4 or IPv6 template is supported for exporting flow monitoring records.

  - User-defined or special templates are not supported for exporting flow monitoring records.

- On all branch SRX Series and J Series devices, flow monitoring IPv6 version 9 has the following limitations:

  - MPLS in not supported.

  - User-defined version 9 templates are not supported.

  - Routing Engine based flow monitoring version 9 is not supported.

  - Flow monitoring and accounting are not supported in chassis cluster mode.

  - Flow monitoring and accounting are not supported on an ae interface.

  - J-Web for IPv6 sampled packets is not supported.

  - SNMP queries for IPv6 sampled packets are not supported

  - Flow monitoring can be configured in version 5, version 8, or version 9 export mode. Up to eight version 9 collectors are supported in export mode.

  - Scope of accounting of IPv6 flow monitoring version 9 packets associated with pseudointerfaces (such as IRB, ML, LAG, VLAN, and GRE) is not supported.

  - Creation of an SCTP session (parallel to TCP) between an exporter and a collector for gathering flow monitoring information is not supported.

- Maximum flow sessions that might be supported include:

  - A device with 1-GB RAM, such as an SRX220 device, might support up to 15,000 flow monitoring sessions at a time.

  - A device with 2-GB RAM, such as an SRX650 device, might support up to 59,900 flow monitoring sessions at a time.

  - Changes in source AS and destination AS are not immediately reflected in exported flows.

- On all branch SRX Series devices, IPv6 traffic transiting over IPv4 based IP over IP tunnel (for example, IPv6-over-IPv4 using ip-x/x/x interface) is not supported.

- The ATM interface takes more than 5 minutes to come up when CPE is configured in ANSI-DMT mode and CO is configured in automode. This occurs only with ALU 7300 DSLAM, due to limitation in current firmware version running on the ADSL Mini-PIM.

- On SRX650 devices, you can only create a maximum of 63 physical interface devices with 1-GB RAM capacity. Therefore, we recommend that you use only 7-octal serial cards to create physical interface devices. To optimally use the 8-octal serial cards, and to create 64 physical interface devices, you require an SRX650 device with 2-GB RAM capacity.

- On SRX100 and J Series devices, dynamic VLAN assignments and guest VLANs are not supported.

- On all branch SRX Series devices, the subnet directed broadcast feature is not supported.

- On SRX650 devices, Ethernet switching is not supported on Gigabit Ethernet interfaces (ge-0/0/0 through ge-0/0/3 ports).

- On SRX210, SRX220, SRX240, and SRX650 devices, logs cannot be sent to NSM when logging is configured in the stream mode. Logs cannot be sent because the security log does not support configuration of the source IP address for the fxp0 interface and the security log destination in stream mode cannot be routed through the fxp0 interface. This implies that you cannot configure the security log server in the same subnet as the fxp0 interface and route the log server through the fxp0 interface.

- On all branch SRX Series devices, the number of child interfaces per node is restricted to 4 on the reth interface and the number of child interfaces per reth interface is restricted to 8.

- On SRX240 High Memory devices, traffic might stop between the SRX240 device and the Cisco switch due to link mode mismatch. We recommend setting the same value to the autonegotiation parameters on both ends.

- On SRX100 devices, the link goes down when you upgrade FPGA on 1xGE SFP. As a workaround, run the **restart fpc** command and restart the FPC.

- On SRX210 devices with VDLS2, ATM COS VBR-related functionality cannot be tested.

- On SRX210 devices, IGMPv2 JOINS messages are dropped on an IRB interface. As a workaround, enable IGMP snooping to use IGMP over IRB interfaces.

- On all J Series devices, the DS3 interface does not have an option to configure multilink-frame-relay-uni-nni (MFR).

- On SRX210, SRX220, and SRX240 devices, every time the VDSL2 Mini-PIM is restarted in the ADSL mode, the first packet passing through the Mini-PIM is dropped.

- On SRX240 Low Memory devices and SRX240 High Memory devices, the RPM server operation does not work when the probe is configured with the option **destination-interface**.

- On all J Series devices, LLDP is not supported on routed ports.

- In J Series xDSL PIMs, mapping between IP CoS and ATM CoS is not supported. If the user configures IP CoS in conjunction with ATM CoS, the logical interface level shaper matching the ATM CoS rate must be configured to avoid congestion drops in segmentation and reassembly (SAR) as shown in the following example:

  ```
  set interfaces at-5/0/0 unit 0 vci 1.110
  set interfaces at-5/0/0 unit 0 shaping cbr 62400 ATM COS
  set class-of-service interfaces at-5/0/0 unit 0 scheduler-map sche_map IP COS
  set class-of-service interfaces at-5/0/0 unit 0 shaping-rate 62400 ADD IFL SHAPER
  ```

- On SRX210, SRX220, and SRX240 devices, the 1-Port Gigabit Ethernet SFP Mini-PIM does not support switching.

- On SRX650 devices, MAC pause frame and FCS error frame counters are not supported for the interfaces ge-0/0/0 through ge-0/0/3.

- On SRX240 and SRX650 devices, the VLAN range from 3967 to 4094 falls under the reserved VLAN address range, and the user is not allowed any configured VLANs from this range.

- On SRX650 devices, the last four ports of a 24-Gigabit Ethernet switch GPIM can be used either as RJ-45 or small form-factor pluggable transceiver (SFP) ports. If both are present and providing power, the SFP media is preferred. If the SFP media is removed or the link is brought down, then the interface will switch to the RJ-45 medium. This can take up to 15 seconds, during which the LED for the RJ-45 port might go on and off intermittently. Similarly, when the RJ-45 medium is active and an SFP link is brought up, the interface will transition to the SFP medium, and this transition could also take a few seconds.

- On SRX210 devices, the USB modem interface can handle bidirectional traffic of up to 19 Kbps. On oversubscription of this amount (that is, bidirectional traffic of 20 Kbps or above), keepalives do not get exchanged, and the interface goes down.

- On SRX100, SRX210, SRX240, and SRX650 devices, on the Layer 3 ae interface, the following features are not supported:

  - Encapsulations (such as CCC, VLAN CCC, VPLS, and PPPoE)

  - J-Web

  - 10-Gigabit Ethernet

- On SRX100 devices, the multicast data traffic is not supported on IRB interfaces.

- On SRX240 High Memory devices, when the **system login deny-sources** statement is used to restrict the access, it blocks a remote copy between nodes, which is used to copy the configuration during the commit routine. Use a firewall filter on the lo0.0 interface to restrict the Routing Engine access, However, if you choose to use the **system login deny-sources** statement, check the private addresses that were automatically on lo0.x and sp-0/0/0.x and exclude them from the denied list.

- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, on VLAN-tagged routed interfaces, LLDP is not supported.

- On SRX210 devices, the DOCSIS Mini-PIM delivers speeds up to a maximum of 100 Mbps throughput in each direction.

- On SRX550 and SRX650 devices, the aggregate Ethernet (ae) interface with XE member interface cannot be configured with the Ethernet switching family.

- On all branch SRX Series and J Series devices, the Q-in-Q support on a Layer 3 interface has the following limitations:

  - Double tagging is not supported on reth and ae interfaces.

  - Multitopology routing is not supported in flow mode and in chassis clusters.

  - Dual tagged frames are not supported on encapsulations (such as CCC, TCC, VPLS, and PPPoE).

  - On Layer 3 logical interfaces, input-vlan-map, output-vlan-map, inner-range, and inner-list are not applicable

  - Only TPIDs with 0x8100 are supported, and the maximum number of tags is 2.

  - Dual tagged frames are accepted only for logical interfaces with IPV4 and IPv6 families.

- On SRX650 devices, LLDP is not supported on the base ports of the device and on the 2-Port 10 Gigabit Ethernet XPIM.

- On SRX100, SRX110, SRX210, SRX220, SRX240, and SRX550 devices, LACP is not supported on the 1-Port Gigabit Ethernet SFP Mini-PIM.

- On all branch SRX Series devices, IKEv2 does not include support for:

  - Policy-based tunnels

  - Dial-up tunnels

  - NAT-T

  - VPN monitoring

  - NHTB for st0—Reusing the same tunnel interface for multiple tunnels

  - EAP

  - Multiple child SAs for the same traffic selectors for each QoS value

  - Proposal enhancement features

  - Reuse of DH exponentials

  - Configuration payloads

- IP Payload Compression Protocol (IPComp)

- Dynamic endpoint (DEP) VPN

Intrusion Detection and Prevention (IDP)

- On all branch SRX Series devices, from Junos OS Release 11.2 and later, the IDP security package is based on the Berkeley database. Hence, when the Junos OS image is upgraded from Junos OS Release 11.1 or earlier to Junos OS Release 11.2 or later, a migration of IDP security package files needs to be performed. This is done automatically on upgrade when the IDP process comes up. Similarly, when the image is downgraded, a migration (secDb install) is automatically performed when the IDP process comes up, and previously installed database files are deleted.

  However, migration is dependent on the XML files for the installed database present on the device. For first-time installation, completely updated XML files are required. If the last update on the device was an incremental update, migration might fail. In such a case, you have to manually download and install the IDP security package using the **download** or **install** CLI command before using the IDP configuration with predefined attacks or groups.

  As a workaround, use the following CLI commands to manually download the individual components of the security package from the Juniper Security Engineering portal and install the full update:

  - **request security idp security-package download full-update**

  - **request security idp security-package install**

- On all branch SRX Series devices, IDP does not allow header checks for nonpacket contexts.

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the maximum supported number of entries in the ASC table is 100,000 entries. Because the user land buffer has a fixed size of 1 MB as a limitation, the table displays a maximum of 38,837 cache entries.

- The maximum number of IDP sessions supported is 16,384 on SRX210 devices, 32,768 on SRX240 devices, and 131,072 on SRX650 devices.

- On all branch SRX Series devices, all IDP policy templates are supported except All Attacks. There is a 100 MB policy size limit for integrated mode and a 150 MB policy size limit for dedicated mode. The current supported IDP policy templates are dynamic based on the attack signatures added. Therefore, be aware that supported templates might eventually grow past the policy size limit.

  On all branch SRX Series devices, the following IDP policies are supported:

  - DMZ_Services

  - DNS_Service

  - File_Server

  - Getting_Started

- IDP_Default

- Recommended

- Web_Server

- On all branch SRX Series devices, IDP deployed in both active/active and active/passive chassis clusters has the following limitations:

  - No inspection of sessions that fail over or fail back.

  - The IP action table is not synchronized across nodes.

  - The Routing Engine on the secondary node might not be able to reach networks that are reachable only through a Packet Forwarding Engine.

  - The SSL session ID cache is not synchronized across nodes. If an SSL session reuses a session ID and it happens to be processed on a node other than the one on which the session ID is cached, the SSL session cannot be decrypted and will be bypassed for IDP inspection.

- On all branch SRX Series devices, IDP deployed in active/active chassis clusters has a limitation that for time-binding scope source traffic, if attacks from a source (with more than one destination) have active sessions distributed across nodes, then the attack might not be detected because time-binding counting has a local-node-only view. Detecting this sort of attack requires an RTO synchronization of the time-binding state that is not currently supported.

  NOTE: **On SRX100 devices, IDP chassis cluster is supported in active/backup mode.**

IPv6

- **Network and Security Manager (NSM)**—Consult the NSM release notes for version compatibility, required schema updates, platform limitations, and other specific details regarding NSM support for IPv6 addressing on SRX Series and J Series devices.

J-Web

- **SRX Series and J Series browser compatibility**

  - To access the J-Web interface, your management device requires the following software:

    - Language support—English-version browsers

    - Supported OS—Microsoft Windows XP Service Pack 3

- Supported browsers

Device	Application	Supported Browsers	Recommended Browser
SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650	J–Web	- Mozilla Firefox version 3.x - Microsoft Internet Explorer version 7.0 NOTE: The New Setup wizard and the PPPoE wizard work best with Mozilla Firefox version 15.x or later.	Mozilla Firefox version 3.x

- To use the Chassis View, a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9) must be installed. Also note that the Chassis View is displayed by default on the Dashboard page. You can enable or disable it using options in the Dashboard Preference dialog box, but clearing cookies in Microsoft Internet Explorer also causes the Chassis View to be displayed.

- On all branch SRX Series devices, in the J–Web interface, there is no support for changing the T1 interface to an E1 interface or vice versa. As a workaround, use the CLI to convert from T1 to E1 and vice versa.

- On all branch SRX Series and J Series devices, users cannot differentiate between Active and Inactive configurations on the System Identity, Management Access, User Management, and Date & Time pages.

- On SRX210 devices, there is no maximum length when the user commits the hostname in CLI mode; however, only 58 characters, maximum, are displayed in the J–Web System Identification panel.

- On all J Series devices, some J–Web pages for new features (for example, the Quick Configuration page for the switching features on J Series devices) display content in one or more modal pop-up windows. In the modal pop-up windows, you can interact only with the content in the window and not with the rest of the J–Web page. As a result, online Help is not available when modal pop-up windows are displayed. You can access the online Help for a feature only by clicking the Help button on a J–Web page.

- On all branch SRX Series devices, you cannot use J–Web to configure a VLAN interface for an IKE gateway. VLAN interfaces are not currently supported for use as IKE external interfaces.

The PPPoE wizard has the following limitations:

- While you use the load and save functionality, the port details are not saved in the client file.

- The Non Wizard connection option cannot be edited or deleted through the wizard. Use the CLI to edit or delete the connections.

- The PPPoE wizard cannot be launched if the backend file is corrupted.

- The PPPoE wizard cannot be loaded from the client file if non-wizard connections share the same units.

- The PPPoE wizard cannot load the saved file from one platform to another platform.

- There is no backward compatibility between PPPoE wizard Phase 2 to PPPoE wizard Phase 1. As a result, the PPPoE connection from Phase 2 will not be shown in Phase 1 when you downgrade to an earlier release.

The New Setup wizard has the following limitations:

- The Existing Edit mode might not work as expected if you previously configured the device manually, without using the wizard.

- Edit mode might overwrite outside configurations such as Custom Application, Policy Name, and zone inbound services.

- In create new mode, when you commit your configuration changes, your changes will overwrite the existing configuration.

- VPN and NAT wizards are not compatible with the New Setup wizard; therefore the VPN or NAT wizard configuration will not be reflected in the New Setup wizard or vice versa.

- By default, 2 minutes are required to commit a configuration using the New Setup wizard.

- On SRX650 devices, the default mode configures only the ge-0/0/1 interface under the internal zone.

- You might encounter usability issues if you use Microsoft Internet Explorer version 7 or 8 to launch the New Setup wizard.

- If you refresh your browser after you download the license, the factory mode wizard is not available.

- When you commit the configuration, the underlying Web management interface changes, and you do not receive a response about the commit status.

- Webserver ports 80 (HTTP) and 443 (HTTPS) on the DMZ or internal zone are overshadowed if Web management is enabled on the Internet zone not configured for destination NAT. As a workaround, change the webserver port numbers for HTTP and HTTPS by editing the recommended policies on the Security policies page.

- Images, buttons, and spinner (indicating that the configuration is being applied) on the wizard screen do not initially appear when the browser cache is cleared.

Layer 2 Transparent Mode

- DHCP server propagation is not supported in Layer 2 transparent mode.

Network Address Translation (NAT)

- **Single IP address in a source NAT pool without PAT**—The number of hosts that a source NAT pool without PAT can support is limited to the number of addresses in the pool. When you have a pool with a single IP address, only one host can be supported, and traffic from other hosts is blocked because there are no resources available.

  If a single IP address is configured for a source NAT pool without PAT when NAT resource assignment is not in active-backup mode in a chassis cluster, traffic through node 1 will be blocked.

- For all ALG traffic, except FTP, we recommend that you not use the static NAT rule options **source-address** or **source-port**. Data session creation can fail if these options are used, because the IP address and the source port value, which is a random value, might not match the static NAT rule. For the same reason, we also recommend that you not use the source NAT rule option **source-port** for ALG traffic.

  For FTP ALG traffic, the **source-address** option can be used because an IP address can be provided to match the source address of a static NAT rule.

  Additionally, because static NAT rules do not support overlapping addresses and ports, they should not be used to map one external IP address to multiple internal IP addresses for ALG traffic. For example, if different sites want to access two different FTP servers, the internal FTP servers should be mapped to two different external IP addresses.

- Maximum capacities for source pools and IP addresses have been extended on SRX650 devices, as follows:

Devices	Source NAT Pools	PAT Maximum Address Capacity	Pat Port Number	Source NAT Rules Number
SRX650 (High Memory devices)	1024	1024	64M	1024
SRX650 (Low Memory devices)	256	256	16M	1024

  Increasing the capacity of source NAT pools consumes memory needed for port allocation. When source NAT pool and IP address limits are reached, port ranges should be reassigned. That is, the number of ports for each IP address should be decreased when the number of IP addresses and source NAT pools is increased. This ensures NAT does not consume too much memory. Use the **port-range** statement in configuration mode in the CLI to assign a new port range or the **pool-default-port-range** statement to override the specified default.

  Configuring port overloading should also be done carefully when source NAT pools are increased.

For source pool with PAT in range (63,488 through 65,535), two ports are allocated at one time for RTP/RTCP applications, such as SIP, H.323, and RTSP. In these scenarios, each IP address supports PAT, occupying 2048 ports (63,488 through 65,535) for ALG module use.

- **NAT rule capacity change**—To support the use of large-scale NAT at the edge of the carrier network, the device-wide NAT rule capacity has been changed.

  The number of destination and static NAT rules has been incremented as shown in Table 2 on page 38. The limitation on the number of destination-rule-set and static-rule-set has been increased.

  Table 2 on page 38 provides the requirements per device to increase the configuration limitation as well as to scale the capacity for each device.

Table 2: Number of Rules on SRX Series and J Series Devices

NAT Rule Type	SRX100	SRX210	SRX240	SRX650	J Series
Source NAT rule	512	512	1024	1024	512
Destination NAT rule	512	512	1024	1024	512
Static NAT rule	512	512	1024	6144	512

The restriction on the number of rules per rule set has been increased so that there is only a device-wide limitation on how many rules a device can support. This restriction is provided to help you better plan and configure the NAT rules for the device.

- On all branch SRX Series devices, in case of SSL proxy, sessions are whitelisted based on the actual IP address and not on the translated IP address. Because of this, in the whitelist configuration of the SSL proxy profile, the actual IP address should be provided and not the translated IP addresses.

  Example:

  Consider a destination NAT rule that translates destination IP address 20.20.20.20 to 5.0.0.1 using the following commands:

  - **set security nat destination pool d1 address 5.0.0.1/32**

  - **set security nat destination rule-set dst-nat rule r1 match destination-address 20.20.20.20/32**

  - **set security nat destination rule-set dst-nat rule r1 then destination-nat pool d1**

  In the above scenario, to exempt a session from SSL proxy inspection, the following IP address should be added to the whitelist:

  - **set security address-book global address ssl-proxy-exempted-addr 20.20.20.20/32**

  - **set services ssl proxy profile ssl-inspect-profile whitelist ssl-proxy-exempted-addr**

Power over Ethernet (PoE)

- On SRX210-PoE devices, SDK packages might not work.

Security Policies

- On all branch SRX Series devices, the current SSL proxy implementation has the following connectivity limitations:

  - The SSLv2 protocol is not supported. SSL sessions using SSLv2 are dropped.

  - SSL sessions where client certificate authentication is mandatory are dropped.

  - SSL sessions where renegotiation is requested are dropped.

- On all branch SRX Series devices, for a particular session, the SSL proxy is only enabled if a relevant feature related to SSL traffic is also enabled. Features that are related to SSL traffic are IDP, application identification, application firewall, and application tracking. If none of the above listed features are active on a session, the SSL proxy bypasses the session and logs are not generated in this scenario.

- On all branch SRX Series and J Series devices, you cannot configure the following IP addresses as negated addresses in a policy:

  - Wildcard addresses

  - IPv6 addresses

  - Addresses such as any, any-ipv4, any-IPv6, and 0.0.0.0

- When a range of addresses or a single address is negated, it can be divided into multiple addresses. These negated addresses are shown as a prefix or a length that requires more memory for storage on a Packet Forwarding Engine.

- Each platform has a limited number of policies with negated addresses. A policy can contain 10 source or destination addresses. The capacity of the policy depends on the maximum number of policies that the platform supports.

- J Series devices do not support the authentication order **password radius** or **password ldap** in the **edit access profile** *profile-name* **authentication-order** command. Instead, use **order radius password** or **ldap password**.

Simple Network Management Protocol (SNMP)

- On all J Series devices, the SNMP NAT related MIB is not supported.

Switching

- **Layer 2 transparent mode support**—On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the following features are not supported for Layer 2 transparent mode:

  - G-ARP on the Layer 2 interface

  - STP

- IP address monitoring on any interface

- Transit traffic through IRB

- IRB interface in a routing instance

- Chassis clustering

- IRB interface handling of Layer 3 traffic

    > **NOTE:** The IRB interface is a pseudointerface and does not belong to the reth interface and redundancy group.

- On SRX100, SRX210, SRX240, and SRX650 devices, change of authorization is not supported with 802.1x.

- On SRX100, SRX210, SRX240, and SRX650 devices, on the routed VLAN interface, the following features are not supported:

    - IPv6 (family inet6)

    - IS-IS (family ISO)

    - Class of service

    - Encapsulations (Ether CCC, VLAN CCC, VPLS, PPPoE, and so on) on VLAN interfaces

    - CLNS

    - PIM

    - DVMRP

    - VLAN interface MAC change

    - G-ARP

    - Change VLAN-Id for VLAN interface

Unified Threat Management (UTM)

- The quarantine action is supported only for UTM Enhanced Web Filtering or Juniper enhanced type of Web filtering.

Upgrade and Downgrade

- On all J Series devices, the Junos OS upgrade might fail due to insufficient disk space if the CompactFlash is smaller than 1 GB in size. We recommend using a 1-GB compact flash for Junos OS Release 10.0 and later.

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, when you connect a client running Junos Pulse 1.0 to an SRX Series device that is a running a later version of Junos Pulse, the client will not be upgraded automatically to the later version. You must uninstall Junos Pulse 1.0 from the client and then download the later version of Junos Pulse from the SRX Series device.

USB

- On all branch SRX Series devices, frequent plug and play of USB keys is not supported. You must wait for the device node creation before removing the USB key.

Virtual Private Networks (VPNs)

The IPv6 IPsec VPN implementation has the following limitations:

- Devices with IPv6 addressing do not perform fragmentation. IPv6 hosts should either perform path MTU discovery or send packets smaller than the IPv6 minimum MTU size of 1280 bytes.

- Because IPv6 addresses are 128 bits long compared to IPv4 addresses, which are 32-bits long, IPv6 IPsec packet processing requires more resources. Therefore, a small performance degradation is observed.

- The IPv6 IPsec VPN does not support the following functions:

  - Remote Access—XAuth, config mode, and shared IKE identity with mandatory XAuth

  - IKE authentication—PKI or DSA

  - IKE peer type—Dynamic IP

  - NAT-T

  - VPN monitoring

  - NHTB

  - SNMP for IPsec VPN MIBs

  - IPv6 link-local address

See *VPN Feature Support for IPv6 Addresses* for more information about IPv6 address support in VPN features.

On all branch SRX Series devices, when you enable VPN, overlapping of the IP addresses across virtual routers is supported with following limitations:

- An IKE external interface address cannot overlap with any other virtual router.

- An internal/trust interface address can overlap across virtual routers.

- An st0 interface address cannot overlap in route-based VPN in point-to-multipoint tunnels such as NHTB.

- An st0 interface address can overlap in route-based VPN in point-to-point tunnels.

SRX100, SRX210, and SRX240 devices have the following limitations:

- The IKE configuration for the Junos Pulse client does not support the hexadecimal preshared key.

- The Junos Pulse client IPsec does not support the AH protocol and the ESP protocol with NULL authentication.

- When you log in through the Web browser (instead of logging in through the Junos Pulse client) and a new client is available, you are prompted for a client upgrade even if the **force-upgrade** option is configured. Conversely, if you log in using the Junos Pulse client with the **force-upgrade** option configured, the client upgrade occurs automatically (without a prompt).

- On all branch SRX Series devices, when you download the Pulse client using the Mozilla browser, the "Launching the VPN Client" page is displayed when Junos Pulse is still downloading. However, when you download the Pulse client using Microsoft Internet Explorer, the "Launching the VPN Client" page is displayed after Junos Pulse has been downloaded and installed.

- On SRX100, SRX210, SRX240, and SRX650 devices, while configuring dynamic VPN using the Junos Pulse client, when you select the authentication-algorithm as sha-256 in the IKE proposal, the IPsec session might not get established.

Unsupported CLI

Dynamic Profiles Hierarchy

- On all branch SRX Series and all J Series devices, the following Firewall hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set dynamic-profiles interfaces interface container-options container-type aps
 fast-aps-switch

set dynamic-profiles interfaces interface fastether-options no-source-filtering

set dynamic-profiles interfaces interface fastether-options source-filtering

set dynamic-profiles interfaces interface services-options close-timeout

set dynamic-profiles interfaces interface services-options fragment-limit

set dynamic-profiles interfaces interface services-options reassembly-timeout

set dynamic-profiles interfaces interface sonet-options aps fast-aps-switch

set dynamic-profiles interfaces interface-range container-options container-type
 aps fast-aps-switch

set dynamic-profiles interfaces interface-range fastether-options
no-source-filtering

set dynamic-profiles interfaces interface-range fastether-options
source-filtering

set dynamic-profiles interfaces interface-range services-options close-timeout

set dynamic-profiles interfaces interface-range services-options fragment-limit

set dynamic-profiles interfaces interface-range services-options
reassembly-timeout

set dynamic-profiles interfaces interface-range sonet-options aps fast-aps-switch

set dynamic-profiles profile-variable-set junos-action-profile

set dynamic-profiles profile-variable-set junos-ccm-interval

set dynamic-profiles profile-variable-set junos-loss-threshold

set dynamic-profiles profile-variable-set junos-ma-name-format
```

```
set dynamic-profiles profile-variable-set junos-md-name-format
```

Interfaces Hierarchy

- On all branch SRX Series and all J Series devices, the following interface hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces interface container-options container-type aps fast-aps-switch

set interfaces interface fastether-options no-source-filtering

set interfaces interface fastether-options source-filtering

set interfaces interface services-options close-timeout

set interfaces interface services-options fragment-limit

set interfaces interface services-options reassembly-timeout

set interfaces interface sonet-options aps fast-aps-switch

set interfaces interface-range container-options container-type aps
fast-aps-switch

set interfaces interface-range fastether-options no-source-filtering

set interfaces interface-range fastether-options source-filtering

set interfaces interface-range services-options close-timeout

set interfaces interface-range services-options fragment-limit

set interfaces interface-range services-options reassembly-timeout

set interfaces interface-range sonet-options aps fast-aps-switch
```

Logical Systems Hierarchy

- On all branch SRX Series and all J Series devices, the following interface hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set logical-systems protocols pim dense-groups dynamic-reject

set logical-systems protocols pim dense-groups pim-dense-group-type

set logical-systems protocols pim dense-groups pim-dense-group-type announce

set logical-systems protocols pim dense-groups pim-dense-group-type name

set logical-systems protocols pim dense-groups pim-dense-group-type reject

set logical-systems routing-instances instance protocols l2vpn associate-profile

set logical-systems routing-instances instance protocols l2vpn associate-profile
 profile-name

set logical-systems routing-instances instance protocols l2vpn associate-profile
 profile-variable-set

set logical-systems routing-instances instance protocols l2vpn mesh-group
associate-profile

set logical-systems routing-instances instance protocols l2vpn mesh-group
associate-profile profile-name

set logical-systems routing-instances instance protocols l2vpn mesh-group
associate-profile profilevariable-set
```

```
set logical-systems routing-instances instance protocols l2vpn mesh-group
mac-flush

set logical-systems routing-instances instance protocols l2vpn mesh-group
mac-flush any-interface

set logical-systems routing-instances instance protocols l2vpn mesh-group
mac-flush any-spoke

set logical-systems routing-instances instance protocols l2vpn mesh-group
mac-flush propagate

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor associate-profile

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor associate-profile profile-name

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor associate-profile profile-variable-set

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor community

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor name

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor psn-tunnel-endpoint

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor standby

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor static

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor static incoming-label

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor backup-neighbor static outgoing-label

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor community

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor connection-protection

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor encapsulation-type

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor ignoreencapsulation-mismatch

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor name

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor pseudowirestatus-tlv

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor psn-tunnelendpoint
```

```
set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor revert-time

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor static

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor static
incoming-label

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor static
outgoing-label

set logical-systems routing-instances instance protocols l2vpn mesh-group
neighbor switchover-delay

set logical-systems routing-instances instance protocols l2vpn mesh-group
route-distinguisher

set logical-systems routing-instances instance protocols l2vpn mesh-group
route-distinguisher rd-type

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-export

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-import

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-target

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-target community

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-target export

set logical-systems routing-instances instance protocols l2vpn mesh-group
vrf-target import

set logical-systems routing-instances instance protocols l2vpn neighbor
associate-profile

set logical-systems routing-instances instance protocols l2vpn neighbor
associate-profile
profile-name

set logical-systems routing-instances instance protocols l2vpn neighbor
associate-profile profilevariable-set

set logical-systems routing-instances instance protocols pim dense-groups
dynamic-reject

set logical-systems routing-instances instance protocols pim dense-groups
pim-dense-group-type

set logical-systems routing-instances instance protocols pim dense-groups
pim-dense-group-type announce

set logical-systems routing-instances instance protocols pim dense-groups
pim-dense-group-type
name

set logical-systems routing-instances instance protocols pim dense-groups
pim-dense-group-type reject

set logical-systems routing-instances instance protocols vpls associate-profile
```

```
set logical-systems routing-instances instance protocols vpls associate-profile
 profile-name

set logical-systems routing-instances instance protocols vpls associate-profile
 profile-variable-set

set logical-systems routing-instances instance protocols vpls mesh-group
associate-profile

set logical-systems routing-instances instance protocols vpls mesh-group
associate-profile
profile-name

set logical-systems routing-instances instance protocols vpls mesh-group
associate-profile profilevariable-set

set logical-systems routing-instances instance protocols vpls mesh-group
mac-flush

set logical-systems routing-instances instance protocols vpls mesh-group
mac-flush any-interface

set logical-systems routing-instances instance protocols vpls mesh-group
mac-flush any-spoke

set logical-systems routing-instances instance protocols vpls mesh-group
mac-flush propagate

set logical-systems routing-instances instance protocols vpls mesh-group neighbor

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 associate-profile

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 associate-profile profile-name

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 associate-profile profile-variable-set

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor community

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor name

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor psn-tunnel-endpoint

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor standby

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor static

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor static incoming-label

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 backup-neighbor static outgoing-label

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 community

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 connection-protection
```

```
set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 encapsulation-type

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 ignore-encapsulation-mismatch

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 name

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 pseudowirestatus-tlv

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 psn-tunnelendpoint

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 revert-time

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 static

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 static
incoming-label

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 static
outgoing-label

set logical-systems routing-instances instance protocols vpls mesh-group neighbor
 switchover-delay

set logical-systems routing-instances instance protocols vpls mesh-group
route-distinguisher

set logical-systems routing-instances instance protocols vpls mesh-group
route-distinguisher rd-type

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-export

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-import

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-target

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-target community

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-target export

set logical-systems routing-instances instance protocols vpls mesh-group
vrf-target import

set logical-systems routing-instances instance protocols vpls neighbor
associate-profile

set logical-systems routing-instances instance protocols vpls neighbor
associate-profile profile-name

set logical-systems routing-instances instance protocols vpls neighbor
associate-profile profile-variable-set

set logical-systems routing-instances instance system services dhcp-local-server
 duplicate-clients-on-interface

set logical-systems routing-instances instance system services dhcp-local-server
 forward-snooped-clients
```

```
set logical-systems routing-instances instance system services dhcp-local-server
 forward-snooped-clients all-interfaces
```

```
set logical-systems routing-instances instance system services dhcp-local-server
 forward-snooped-clients configured-interfaces
```

```
set logical-systems routing-instances instance system services dhcp-local-server
 forward-snooped-clients non-configured-interfaces
```

```
set logical-systems system services dhcp-local-server
duplicate-clients-on-interface
```

```
set logical-systems system services dhcp-local-server forward-snooped-clients
```

```
set logical-systems system services dhcp-local-server forward-snooped-clients
all-interfaces
```

```
set logical-systems system services dhcp-local-server forward-snooped-clients
configured-interfaces
```

```
set logical-systems system services dhcp-local-server forward-snooped-clients
non-configured-interfaces
```

Protocols Hierarchy

- On all branch SRX Series and all J Series devices, the following CLI commands are not supported. However, if you enter these commands in the CLI editor, they will appear to succeed and will not display an error message.

```
set protocols pim dense-groups dynamic-reject
```

```
set protocols pim dense-groups pim-dense-group-type
```

```
set protocols pim dense-groups pim-dense-group-type announce
```

```
set protocols pim dense-groups pim-dense-group-type name
```

```
set protocols pim dense-groups pim-dense-group-type reject
```

Routing Hierarchy

- On all branch SRX Series and all J Series devices, the following routing hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set routing-instances instance protocols l2vpn associate-profile
```

```
set routing-instances instance protocols l2vpn associate-profile profile-name
```

```
set routing-instances instance protocols l2vpn associate-profile
profile-variable-set
```

```
set routing-instances instance protocols l2vpn mesh-group associate-profile
```

```
set routing-instances instance protocols l2vpn mesh-group associate-profile
profile-name
```

```
set routing-instances instance protocols l2vpn mesh-group associate-profile
profile-variable-set
```

```
set routing-instances instance protocols l2vpn mesh-group mac-flush
```

```
set routing-instances instance protocols l2vpn mesh-group mac-flush any-interface
```

```
set routing-instances instance protocols l2vpn mesh-group mac-flush any-spoke
```

```
set routing-instances instance protocols l2vpn mesh-group mac-flush propagate
```

```
set routing-instances instance protocols l2vpn mesh-group neighbor
```

```
set routing-instances instance protocols l2vpn mesh-group neighbor
associate-profile

set routing-instances instance protocols l2vpn mesh-group neighbor
associate-profile profile-name

set routing-instances instance protocols l2vpn mesh-group neighbor
associate-profile profile-variable-set

sset routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor community

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor name

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor psn-tunnel-endpoint

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor standby

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor static

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor static incoming-label

set routing-instances instance protocols l2vpn mesh-group neighbor
backup-neighbor static outgoing-label

set routing-instances instance protocols l2vpn mesh-group neighbor community

set routing-instances instance protocols l2vpn mesh-group neighbor
connection-protection

set routing-instances instance protocols l2vpn mesh-group neighbor
encapsulation-type

set routing-instances instance protocols l2vpn mesh-group neighbor
ignore-encapsulation-mismatch

set routing-instances instance protocols l2vpn mesh-group neighbor name

set routing-instances instance protocols l2vpn mesh-group neighbor
pseudowire-status-tlv

set routing-instances instance protocols l2vpn mesh-group neighbor
psn-tunnel-endpoint

set routing-instances instance protocols l2vpn mesh-group neighbor revert-time

set routing-instances instance protocols l2vpn mesh-group neighbor static

set routing-instances instance protocols l2vpn mesh-group neighbor static
incoming-label

set routing-instances instance protocols l2vpn mesh-group neighbor static
outgoing-label

set routing-instances instance protocols l2vpn mesh-group neighbor
switchover-delay

set routing-instances instance protocols l2vpn mesh-group route-distinguisher

set routing-instances instance protocols l2vpn mesh-group route-distinguisher
rd-type

set routing-instances instance protocols l2vpn mesh-group vrf-export
```

```
set routing-instances instance protocols l2vpn mesh-group vrf-import

set routing-instances instance protocols l2vpn mesh-group vrf-target

set routing-instances instance protocols l2vpn mesh-group vrf-target community

set routing-instances instance protocols l2vpn mesh-group vrf-target export

set routing-instances instance protocols l2vpn mesh-group vrf-target import

set routing-instances instance protocols l2vpn neighbor associate-profile

set routing-instances instance protocols l2vpn neighbor associate-profile
profile-name

set routing-instances instance protocols l2vpn neighbor associate-profile
profile-variable-set

set routing-instances instance protocols pim dense-groups dynamic-reject

set routing-instances instance protocols pim dense-groups pim-dense-group-type

set routing-instances instance protocols pim dense-groups pim-dense-group-type
 announce

set routing-instances instance protocols pim dense-groups pim-dense-group-type
 name

set routing-instances instance protocols pim dense-groups pim-dense-group-type
 reject

set routing-instances instance protocols vpls associate-profile

set routing-instances instance protocols vpls associate-profile profile-name

set routing-instances instance protocols vpls associate-profile
profile-variable-set

set routing-instances instance protocols vpls mesh-group associate-profile

set routing-instances instance protocols vpls mesh-group associate-profile
profile-name

set routing-instances instance protocols vpls mesh-group associate-profile
profile-variable-set

set routing-instances instance protocols vpls mesh-group mac-flush

set routing-instances instance protocols vpls mesh-group mac-flush any-interface

set routing-instances instance protocols vpls mesh-group mac-flush any-spoke

set routing-instances instance protocols vpls mesh-group mac-flush propagate

set routing-instances instance protocols vpls mesh-group neighbor

set routing-instances instance protocols vpls mesh-group neighbor
associate-profile

set routing-instances instance protocols vpls mesh-group neighbor
associate-profile profile-name

set routing-instances instance protocols vpls mesh-group neighbor
associate-profile profile-variable-set

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 community

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 name
```

```
set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 psn-tunnel-endpoint

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 standby

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 static

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 static incoming-label

set routing-instances instance protocols vpls mesh-group neighbor backup-neighbor
 static outgoing-label

set routing-instances instance protocols vpls mesh-group neighbor community

set routing-instances instance protocols vpls mesh-group neighbor
connection-protection

set routing-instances instance protocols vpls mesh-group neighbor
encapsulation-type

set routing-instances instance protocols vpls mesh-group neighbor
ignore-encapsulation-mismatch

set routing-instances instance protocols vpls mesh-group neighbor name

set routing-instances instance protocols vpls mesh-group neighbor
pseudowire-status-tlv

set routing-instances instance protocols vpls mesh-group neighbor
psn-tunnel-endpoint

set routing-instances instance protocols vpls mesh-group neighbor revert-time

set routing-instances instance protocols vpls mesh-group neighbor static

set routing-instances instance protocols vpls mesh-group neighbor static
incoming-label

set routing-instances instance protocols vpls mesh-group neighbor static
outgoing-label

set routing-instances instance protocols vpls mesh-group neighbor
switchover-delay

set routing-instances instance protocols vpls mesh-group route-distinguisher

set routing-instances instance protocols vpls mesh-group route-distinguisher
rd-type

set routing-instances instance protocols vpls mesh-group vrf-export

set routing-instances instance protocols vpls mesh-group vrf-import

set routing-instances instance protocols vpls mesh-group vrf-target

set routing-instances instance protocols vpls mesh-group vrf-target community

set routing-instances instance protocols vpls mesh-group vrf-target export

set routing-instances instance protocols vpls mesh-group vrf-target import

set routing-instances instance protocols vpls neighbor associate-profile

set routing-instances instance protocols vpls neighbor associate-profile
profile-name

set routing-instances instance protocols vpls neighbor associate-profile
profile-variable-set
```

```
set routing-instances instance system services dhcp-local-server
duplicate-clients-on-interface
```

```
set routing-instances instance system services dhcp-local-server
forward-snooped-clients
```

```
set routing-instances instance system services dhcp-local-server
forward-snooped-clients all-interfaces
```

```
set routing-instances instance system services dhcp-local-server
forward-snooped-clients configured-interfaces
```

```
set routing-instances instance system services dhcp-local-server
forward-snooped-clients non-configured-interfaces
```

Security Hierarchy

- On all branch SRX Series and all J Series devices, the following services hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set security idp sensor-configuration application-identification
application-system-cache
```

```
set security idp sensor-configuration application-identification
application-system-cache-timeout
```

```
set security idp sensor-configuration application-identification disable
```

```
set security idp sensor-configuration application-identification max-sessions
```

```
set security idp sensor-configuration application-identification
no-application-system-cache
```

System Hierarchy

- On all branch SRX Series and all J Series devices, the following system hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set system services dhcp-local-server duplicate-clients-on-interface
```

```
set system services dhcp-local-server forward-snooped-clients
```

```
set system services dhcp-local-server forward-snooped-clients all-interfaces
```

```
set system services dhcp-local-server forward-snooped-clients
configured-interfaces
```

```
set system services dhcp-local-server forward-snooped-clients
non-configured-interfaces
```

Related Documentation

- New and Changed Features on page 6

- Changes in Behavior and Syntax on page 15

- Known Issues on page 53

- Resolved Issues on page 57

- Documentation Updates on page 63

- Migration, Upgrade, and Downgrade Instructions on page 70

Known Issues

The following problems currently exist in Juniper Networks branch SRX Series Services Gateways and J Series Services Routers. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

> **NOTE:** For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

Application Layer Gateways (ALGs)

- On SRX Series devices, the REAL ALG is not supported, but you can configure it in both CLI and J-Web. PR943123

Application-Aware Quality of Service (AppQoS)

- When IPsec is enabled, AppQoS does not assign egress traffic to the configured forwarding class. PR753762

- On devices in a chassis cluster Z mode, traffic rate-limited shows deviation in traffic forwarding rate. PR779368

- When IPsec is enabled, AppQoS does not apply the rate limiter for egress traffic. PR918942

- When GRE is enabled, AppQoS classification, marking, or rate limit does not work for fragmented packets in client-to-server direction. PR924932

AppSecure

- AppID might not identify the application during stress traffic conditions for 1-GB memory devices due to insufficient memory.

  As a workaround, use 2-GB memory devices. PR923548

AppSecure

- You cannot apply class of service (CoS) rewrite rules based on AppQoS. PR782050

Chassis Cluster

- On devices in a chassis cluster, the **clear interface stats** command does not work when any of the nodes in a chassis cluster are down. PR550641

- On SRX210, SRX220, and SRX240 devices, the maximum transmission unit (MTU) value on the SRX-MP-1SFP-GE Mini-PIM interface is 9010. If the Mini-PIM interface was configured as a chassis cluster fabric interface, the chassis cluster fabric interface automatically sets the MTU value to 9014 to support jumbo frames. Setting the MTU value fails on the Mini-PIM interface configured as a chassis cluster fabric interface, and the Mini-PIM interface retains the default MTU setting (1514). The packets that

were larger than the 1514-byte frame are dropped because the chassis cluster fabric interface does not support fragmentation.

> NOTE: Prior to Junos OS Release 11.4R1, the SFP interfaces on Mini-PIMs are not supported to be used as fabric link in a chassis cluster.

PR865975

- When Layer 2 bridging is configured, both the nodes must be rebooted. After you reboot the primary node, the secondary node goes into a disabled state because of a fabric link failure.

  As a workaround, reboot both the nodes (including the one running as primary). Rebooting only the disabled node does not resolve the issue. PR892374

- On J Series devices in a chassis cluster, when you manually trigger the restart forwarding on the primary node, the secondary node might get disabled and cannot be recovered back to normal state without rebooting both the nodes. PR895614

- The secondary node in a chassis cluster environment might crash or go into DB mode because of **panic: rnh_index_alloc** after frequent failover when IPsec VPN is enabled. PR917719

- On devices in a chassis cluster, the PIC might go offline on one of the nodes due to RG0 failover caused by rebooting the device. PR933248

Command-Line Interface (CLI)

- On all branch SRX Series devices, in the output of the **show services application-identification application-system-cache** command, the application-system-cache table for P2P encrypted traffic is incorrectly marked as **Encrypted: No instead of Encrypted:Yes**. PR704023

- On SRX210 devices, you cannot configure **0.0.0.0/0 in dialer-options watch-list**. The **set interfaces dl0 unit 0 dialer-options watch-list 0.0.0.0/0** command fails. PR841371

Flow and Processing

- The maximum MTU supported on the 1XGE Mini-PIM card is 9010 bytes for both optical and copper SFP transceiver. If a 1XGE Mini-PIM card is configured with a value greater than 9010, the earlier committed value takes effect, but no error message is displayed in the CLI. However, the log captures the failure to set the configured MTU value. PR825691

- When data flowsets are exported after AS configuration changes, the changes to source AS (srcAS) and destination AS (dstAS) values are not reflected immediately in the exported flows. PR864416

- When sampling is enabled, the **template-refresh-rate** and **option-refresh-rate** options takes into account a default value of 60 seconds, if packets are configured without any value for seconds. PR865413

- When reverse path forwarding (RPF) is enabled along with RPM, the device changes to the db prompt and loses the reach ability when you delete some configurations. PR869528

- On SRX210 and SRX220 devices, when the baseboard port or the 1XGE Mini-PIM port over IRB is configured to receive joins for any valid multicast address x.1.1.1, the multicast address is not recognized and it is not present in the PIM join or IGMP group. PR873909

- On devices with 1 GB of memory, if the advanced services license is configured with the **reduce-dp-memory** option, memory is not released from the data plane to the control plane.

  As a workaround, when the advanced services license is configured, do not configure the **reduce-dp-memory** option. PR895648

- On SRX220H2 devices, the TCP connection rate might drop by 15 percent. PR898217

- The size of ARP response frames is limited. If a received ARP response exceeds this limit, the device drops the response and the counter increases incrementally. PR927387

Hardware

- On SRX550 devices, USB modem is not supported. PR856058

- On the B and H versions of SRX100, SRX210, and SRX240 devices with 1 GB RAM, the predefined IPS templates other than the recommended template might not compile successfully. PR925337

Infrastructure

- When forwarding restarts on the primary node or when the primary node is rebooted, occasionally, the Flexible PIC Concentrator (FPC) on that node might not come online. Multiple reboots of the node are required to bring the FPC online. PR868792

- After installing advance services such as UTM and IDP, the corresponding bit of the NVRAM environment variable **wmem_selector** will be set. This bit is used to decide if the advance service should be enabled or not. PR943672

Interfaces and Routing

- On SRX210 High Memory devices, the state of the cl-0/0/8 interface reflects only the output packets sent but does not show the input packets received over the Dialer interface (dl0). PR662813

- For point-to-point interfaces the RSVP interface state might show as DOWN if the interface configuration is changed while the interface is enabled for RSVP. Different types of configuration changes can trigger this issue including address or MTU changes.

  As a workaround, make any changes to point-to-point interfaces before enabling RSVP on that specific interface. PR772807

- The SHDSL media and statistics counters do not increment after the introduction of micro-interruption to the line. The counters are also not cleared even after explicitly you use the **clear** command. PR810334

- When the Flexible PIC Concentrator (FPC) was removed or made to go offline, the FPC status is not detected. PR818363

- On SRX550 devices, the T3/E3 FPC goes offline after provisioning a switched port. PR919617

- On SRX550 devices with DS3/E3 interfaces, the external clocking option is disabled to support the clocking option. PR936356

Switching

- On all branch SRX Series and J Series devices, LLDP is supported only on interface unit 0. PR553991

- On SRX650 devices in a chassis cluster, when the fabric link is disabled manually using the CLI, the secondary node remains in the secondary mode. As a result, in the active/active mode, the Z-traffic is dropped even when the secondary node is up and the fabric link status is down. PR839193

System Logs

- On all branch SRX Series devices, when the source address is specified for a particular host, eventd core files are generated.

  As a workaround, do not limit the source address to a particular host. PR769855

Unified Threat Management (UTM)

- Invalid notification options are displayed in antivirus fallback-block notification. PR787063

- When both UTM and IDP are configured, the C2S policy cannot be loaded with the latest signature package. If UTM is not configured but the UTM file **-/cf/var/db/qav/qavdb_good.dat** is still present, when you delete the UTM file, the C2S policy will be loaded successfully. To delete the UTM file, use the following command: **request security utm anti-virus juniper-express-engine pattern-delete**. PR869133

- Webpages become unavailable and do not display any content when you enable Sophos antivirus for HTTP traffic.

  As a workaround, use Kaspersky or Express antivirus instead of Sophos antivirus when both antivirus and content filtering are required for HTTP traffic. PR906534

- Before the HTTP 200 OK with chunk-size passes an antivirus engine, it is recognized as an invalid data packet.

  As a workaround, disable the antivirus intelligent prescanning. PR937539

Virtual Private Networks (VPNs)

- When a device is configured to support remote access VPN clients with a local address pool, memory usage of the general authentication service process (authd) increases slowly over time.

As a workaround, execute the **restart general-authentication-service** command to prevent the memory usage from reaching a critical level. PR894232

- Certificate-based authentication would fail when the RSA signature from the remote peer used SHA-256 as the message digest algorithm. PR936141

- After traffic-selector configuration is deleted from the VPN configuration object, the data traffic stops passing through the tunnel.

  As a workaround, after deleting the traffic-selector configuration, execute the commit full command instead of commit. PR944598

Related Documentation

Resolved Issues

The following are the issues that have been resolved in Junos OS Release 12.1X46-D10 for Juniper Networks SRX Series Services Gateways. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

NOTE: For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

Application Layer Gateways (ALGs)

- The total SIP call values were incorrect, and the ALG feature could not be verified. PR839190

- On all branch SRX Series devices in a chassis cluster, the flowd process might crash when the ALG is enabled and the security policy is configured with the **log** option for ALG traffic. PR889097

- The Sun RPC ALG cannot open the gate as expected if the port string in **get-address** message is longer than 6, because current Sun RPC ALG can only parse the **uaddr** port string which is lesser than 6. PR901205

Authentication

- On all branch SRX Series devices configured with firewall authentication, if a user was already authenticated, and then when a subsequent user initiated authentication using the same IP address as the first user, the subsequent user inherited the first authenticated user's "Access time remaining" value. PR843591

Chassis Cluster

- On devices in a chassis cluster, when you execute the **clear system commit** command, it clears commit only from the local node. PR821957

- On devices in a chassis cluster, during a control link failure, if the secondary node is rebooted by control link failure recovery, the rebooted node goes into disabled state even after startup. PR828558

- On all branch SRX Series devices in a chassis cluster, when you download IDP Signature Database from the primary node, the **sig-db** is not synchronized to the secondary node. PR914987

Command-Line Interface (CLI)

- There is no specific CLI command to display the count of sessions allowed, denied, or terminated because of UAC enforcement. PR733995

- AppQoS does not display the correct application identification name when you run the **show class-of-service application-traffic-control statistics rate-limiter** CLI command. PR751490

Dynamic Host Configuration Protocol (DHCP)

- On all branch SRX Series devices, when there are multiple interfaces configured as DHCP client, if one of DHCP client interface is from down state to up state, the IP address acquired by other DHCP client interfaces will be deleted unexpectedly and are added back after sometime. There is temporary traffic interruption until the deleted IP address is recovered automatically. PR890124

- Prior to Junos OS Release 11.4R9, DHCP option 125 cannot be configured for use as the **byte-stream** option. With Junos OS Release 11.4R9 and later releases, DHCP option 125 can be used for the **byte-stream** option. PR895055

- On all branch SRX Series devices working as DHCP clients, when the connection with the primary DHCP server is lost, the device tries to renew the lease. The device then drops the DHCP rebind ACK from the other DHCP server, which tries to assign the same IP address to it. PR911864

Flow and Processing

- When DNS ALG was enabled, the rewrite rules applied on the egress interface might not work for DNS messages. PR785099

- After enabling IPv6 in flow mode, IPv6 routes are not active. PR824563

- Current implementation of timeout for http is 1800s, the default timeout should be 300s. PR858621

- The RPM script triggers twice when the RPM probe-test fails. PR869519

- On J Series devices, the self-originating outbound traffic always uses the first logical unit queue. PR887283

- On all branch SRX Series devices with the MS-RPC ALG enabled, when the **junos-ms-rpc** application is not configured in the security policy and if the MS RPC control session is permitted by the security policy that matched the application "any", then the MS-RPC ALG should not check the MS RPC data session and be permitted by the security policy. If the MS-RPC data session is configured to be processed by one or more other services such as IDP, UTM, AppID, or AppFW, then the MS-RPC ALG incorrectly checks the MS RPC data session and discards the MS RPC data session. PR904682

- On SRX100, SRX110, SRX210, and SRX220 devices with the FTP Application Layer Gateway (ALG) enabled, ICMP redirect might not work for FTP traffic. PR904686

- The memory allocated for multicast session might not release when multicast reroute occurs, this leads to memory leak. PR905375

- When you use a classifier based on EXP bits on a PE router, the CoS marked MPLS traffic is forwarded to the default egress queues instead of the custom configured queues. PR920066

Hardware

- On SRX210 devices, after you upgrade to Junos OS 12.1X46-D10 or later, the fan speed in relation to the Routing Engine temperature does not follow the temperature threshold table. PR910977

Infrastructure

- On all branch SRX Series devices, when the device authentication is through RADIUS server and the password protocol is Microsoft CHAP version 2, the password change operation fails as the user password change is enforced through Microsoft Active Directory server. PR740869

- After an upgrade, you cannot copy files between nodes in a cluster using the **file copy** command. PR817228

- On SRX240 devices, when a nonstandard HTTPS port is set, the URI changes to the IP address and port. PR851741

- On SRX100B and SRX100H devices unexpected system reboot is observed, and multiple core files are generated due to a double data rate2 (DDR2) memory timing issue between DRAM and CPU. The symptoms include flowd core files, core files from other daemons (such as snmpd, ntpd, rtlogd and so on) and silent reboot without core files are generated. These core files are related to random memory access (example: pointer corruption in session ager ring entry). PR909069

Interfaces and Routing

- The Routing Protocol Daemon (RPD) might crash with the following error: **/kernel: BAD_PAGE_FAULT: pid 1472 (rpd), uid 0: pc 0x86ff81c got a read fault at 0x15,x86 fault flags = 0x4**, when the OSPF switches from the primary path to the secondary path when loop-free alternates (LFA) and LDP-SYNC are enabled. The corruption is caused when OSPF does not completely free a memory location that is later reused by LDP. PR737141

- On VLAN tagged ethernet frames (802.1p), you cannot modify the VDSL priority bits. PR817939

- On SRX550 devices, the VRRP does not work when it is connected through IRB. PR834766

- On J Series devices, a Layer 2 loop might occur for a short time when you run the **request system power-off**, **request system reboot**, or **request system halt** command. PR856457

- The RPM script is triggered twice when the RPM probe-test fails. PR869519

- When a SHDSL Mini-PIM is configured in 2-wire mode with annex mode as Annex B/G, one of the physical interfaces does not come up. PR874249, PR882035

- The point-to-multipoint (P2MP) interface does not accept any multicast packets, this leads to interoperability issues with the Secure Services Gateway (SSG). PR895090

- When there is a configuration change in the VDSL profile from one to another, the VDSL line does not retrain and comes up with the newly configured VDSL profile. PR898775

- When the virtual routers (routing instances) are connected with a looped cable and if one of the interfaces is VLAN, the unicast communication is unsuccessful. PR909190

- When multiple routing-instances are defined, DNS names in the address-book entries might not get resolved. This results in corresponding security policies to be nonoperational. PR919810

J-Web

- On SRX550 devices, the "External storage" option is not supported. Hence, do not select the "External storage" option from the list on the **Maintain > reboot** and **snapshot** page. PR741593

- The J-Web interface was vulnerable to HTML cross-site scripting attacks, also called XST or cross-site tracing. PR752398

- The Layer 2 Transparent Mode feature does not work with group configurations. PR815225

- In J-Web, if the policy name was "0", the penultimate-hop popping (PHP) function treated it as empty, and traffic log output could not be viewed. PR853093

- J-Web fails to display the member in the application set after adding it to the nested application set. PR883391

- On J-Web, when you configure policy, the address set is seen as undefined in the Policy wizard. But, if a policy is created from **Security > Policy > Apply** policy, the address set is seen. PR892766

- On J-Web, the configured maximum flow memory value key **max-flow-mem** is marked as deprecated and hidden. Therefore, the maximum flow memory value cannot be fetched or displayed in J-Web. PR894787

- J-Web fails to display all policies under the from or to zone if one of them has the ## string in the description field. PR917136

License

- On SRX100 High Memory devices, after returning to zero the system licenses are deleted and the device reverts to an SRX100B device. PR863962

Network Address Translation (NAT)

- NAT-T might not work when the VPN is with Cisco and if the VPN is initiated from a Cisco peer. The VPN negotiates using port UDP 500 instead of UDP 4500 when NAT is involved. PR869458

- On devices in a chassis cluster, the chassis cluster rule number of sessions in the SNMP query or walk result is the sum of the real number of sessions of the primary node and the secondary node. PR908206

Switching

- On SRX650 devices, the dot1x:mode:Multiple:Supplicants were authenticated even after a disconnect message was sent from the RADIUS server. PR786731

Unified Threat Management (UTM)

- The antivirus fallback block notification displays invalid notification option. PR787063

- When full file-based scanning of antivirus is enabled with Kaspersky scanning, some websites are not accessible. PR853516

- The flowd process might crash when traffic is processed by UTM. PR854880

- The device tries to resolve and connect to **cpa.surfcpa.com** and **update.juniper-updates.net** even if there are no licenses or configuration related to UTM. PR856128

- On all branch SRX Series devices using EWF, a small percentage of the connections to the Websense Threat Seeker cloud might time out. PR860514

- The EWF parser mishandled URL and hosts from the HTTP header. This results in an uncategorized EWF reply. PR862602

- On all branch SRX Series devices with UTM content filtering configured, a long file name encoded with the ISO-2022 might incorrectly match the content filtering

extension blocking policy even if the extension blocking list does not contain the type of file extension. As a result, the file is dropped. PR865607

- On all branch SRX Series devices, new categories for EWF have been added. PR866160

User Interface and Configuration

- On SRX240 devices (with H2 and B2 model numbers) running Junos OS Release 11.4R8 or 11.4R9, you cannot upgrade to Junos OS Release 11.4R10 or later.

  You can upgrade from Junos OS Release 11.4R8 or 11.4R9 to Junos OS Release 12.1X44-D10, 12.1X45-D10, and 12.1X46-D10. PR934393

Virtual Private Networks (VPNs)

- On an SRX Series device, when a session is closed because the user for that session has signed out from the Junos Pulse, the session close log shows the role information as "N/A". PR689607

- The SRX Series cluster is used as a VPN concentrator that is connected to remote VPN clients. The Internet key exchange process (daemon) tries to reuse the IP address that was previously assigned to an XAuth client. But the IKEd Xauth attributes are overwritten when the authentication reply is received from Authd. This causes the IKEd to assign a new IP address every time a Phase 1 Security Association (SA) is negotiated. As a result, multiple remote clients cannot connect through VPN. PR854922

- On all branch SRX Series devices, the Junos Pulse client has been updated from Release 2.0R3 to 4.0R2. PR868101

- On all branch SRX Series devices, a memory leak occurs on the data plane during continuous interface flapping, such as when interfaces are continuously added or deleted. PR898731

- For IKEv2, if an SRX Series device running Junos OS Release 12.1X46-D10 is in negotiation with a peer SRX Series device running Junos OS Release 11.4 or 12.1X44, a kmd core file might be generated on the peer device during IPsec child SA rekey. This does not impact any IKEv1 scenarios. PR915376

- On all branch SRX Series devices configured with group VPN, the flowd process might crash when group VPN Security Association (SA) rekeys and swaps to the new VPN tunnel. PR925107

Related Documentation

Documentation Updates

This section lists the errata and changes in Junos OS Release 12.1X46-D10 documentation.

Documentation Updates for the Junos OS Software Documentation

This section lists improvements and outstanding issues with the software documentation.

Junos OS for SRX Series Documentation

The Junos OS for SRX Series technical documentation set has been expanded, restructured, and retitled in Junos OS Release 12.1X46-D10 to make it more comprehensive, easy-to-use, and intuitive. Highlights:

- (New) The Complete Software Guide consolidates all of the release-specific content that applies to Junos OS for SRX Series devices (except release notes) into a three volume set of PDFs that you can download and view offline. The first volume contains getting started and administration information; the second contains feature information; the third contains developer information. You can find the PDFs in the Downloads box on the right side of the *Junos OS for SRX Series Services Gateways, Release 12.1X46* index page.

- (New) The *Getting Started Guide for Branch SRX Series* describes how to get up and running with branch SRX Series devices.

- (Expanded) The *Junos OS Monitoring and Troubleshooting Library for Security Devices* contains significantly more content to help network and security managers keep their SRX Series devices running smoothly in their production environments.

- (Expanded) The *Junos OS for SRX Series Services Gateways, Release 12.1X46* index page has been expanded to serve as a "one stop shop" for all of your Junos OS for SRX Series technical documentation needs.

BGP Feature Guide for Security Devices

- In "Example: Configuring Route Authentication for BGP," the following configuration steps in the CLI quick configuration and in the step-by-step procedure sections are not supported on SRX Series devices:

```
set security authentication-key-chains key-chain bgp-auth tolerance 30
set security authentication-key-chains key-chain bgp-auth key 0 secret
this-is-the-secret-password
set security authentication-key-chains key-chain bgp-auth key 0 start-time
2011-6-23.20:19:33-0700
set security authentication-key-chains key-chain bgp-auth key 1 secret
this-is-another-secret-password
set security authentication-key-chains key-chain bgp-auth key 1 start-time
2012-6-23.20:19:33-0700
```

J Series Services Router Advanced WAN Access Configuration Guide

- The example given in the "Configuring Full-Cone NAT" section in the guide available at http://www.juniper.net/techpubs/software/jseries/junos85/index.html is incorrect. The correct and updated example is given in the revised guide available at http://www.juniper.net/techpubs/software/jseries/junos90) .

J2320, J2350, J4350, and J6350 Services Router Getting Started Guide

- The "Connecting to the CLI Locally" section states that the required adapter type is DB-9 female to DB-25 male. This is incorrect; the correct adapter type is DB-9 male to DB-25 male.

J-Web

- **J-Web Security Package Update Help page**—This Help page does not contain information about the download status.

- **J-Web pages for stateless firewall filters**—There is no documentation describing the J-Web pages for stateless firewall filters. To find these pages in J-Web, go to **Configure>Security>Firewall Filters**, and then select **IPv4 Firewall Filters** or **IPv6 Firewall Filters**. After configuring the filters, select **Assign to Interfaces** to assign your configured filters to interfaces.

Modem Interfaces Feature Guide for Security Devices

- The Example: Configuring the 3G Wireless Modem Interface in Modem Interfaces Guide provides the following incorrect information for configuring a dialer filter for the 3G wireless modem interface:

  - user@host# **set firewall family inet dialer-filter corporate-traffic-only term term1 from source-address 20.20.90.4/32**

  - user@host# **set firewall family inet dialer-filter corporate-traffic-only term term1 from destination-address 200.200.201.1/32**

  - user@host# **set firewall family inet dialer-filter corporate-traffic-only term term1 then note**

  The following incorrect configuration output is included:

```
      [edit]
user@host# show firewall family inet dialer-filter corporate-traffic-only
term term1 {
  from {
    source-address {
      20.20.90.4/32;
    }
    destination-address {
      200.200.201.1/32;
    }
  }
  then note;
}
```

The correct configuration is:

user@host# **set firewall family inet dialer-filter corporate-traffic-only term term1 then note**

The following configuration is output from the correct configuration:

```
       [edit]
  user@host# show firewall
  family inet {
    dialer-filter corporate-traffic-only {
      term term-1 {
        then note;
      }
    }
  }
```

Network Address Translation

The command **show security nat source persistent-nat-table** under Network Address Translation > Administration > Source NAT operational commands has the following errors:

- The command is missing the **summary** option—Display persistent NAT bindings summary.

- The command contains incomplete sample output—The corrected sample output is as follows:

show security nat source persistent–nat–table internal-ip internal-port

user@host> **show security nat source persistent–nat–table internal-ip 9.9.9.1 internal-port 60784**

```
Internal                         Reflective        Source      Type
Left_time/  Curr_Sess_Num/ Source
 In_IP  In_Port I_Proto Ref_IP    Ref_Port R_Proto NAT Pool
Conf_time   Max_Sess_Num  NAT Rule
9.9.9.1 60784   udp  66.66.66.68  60784      udp   dynamic-customer-source
any-remote-host  254/300  0/30 105
```

show security nat source persistent–nat–table all

user@host> **show security nat source persistent–nat–table all**

```
 Internal               Reflective                  Source      Type
Left_time/  Curr_Sess_Num/  Source
 In_IP     In_Port I_Proto Ref_IP       Ref_Port R_Proto NAT Pool
    Conf_time   Max_Sess_Num   NAT Rule
9.9.9.1    63893   tcp   66.66.66.68   63893      tcp   dynamic-customer-source
 any-remote-host  192/300   0/30 105
9.9.9.1    64014   udp   66.66.66.68   64014      udp   dynamic-customer-source
 any-remote-host  244/300   0/30 105
9.9.9.1    60784   udp   66.66.66.68   60784      udp   dynamic-customer-source
 any-remote-host  254/300   0/30 105
9.9.9.1    57022   udp   66.66.66.68   57022      udp   dynamic-customer-source
 any-remote-host  264/300   0/30 105
9.9.9.1    53009   udp   66.66.66.68   53009      udp   dynamic-customer-source
 any-remote-host  268/300   0/30 105
9.9.9.1    49225   udp   66.66.66.68   49225      udp   dynamic-customer-source
```

```
                       any-remote-host  272/300   0/30 105
                       9.9.9.1    52150   udp   66.66.66.68   52150   udp   dynamic-customer-source
                       any-remote-host  274/300   0/30 105
                       9.9.9.1    59770   udp   66.66.66.68   59770   udp   dynamic-customer-source
                       any-remote-host  278/300   0/30 105
                       9.9.9.1    61497   udp   66.66.66.68   61497   udp   dynamic-customer-source
                       any-remote-host  282/300   0/30 105
                       9.9.9.1    56843   udp   66.66.66.68   56843   udp   dynamic-customer-source
                       any-remote-host   -/300   1/30 105
```

show security nat source persistent-nat-table summary

```
user@host> show security nat source persistent-nat-table summary
Persistent NAT Table Statistics on FPC5 PIC0:
binding total : 65536
binding in use : 0
enode total : 524288
enode in use : 0
```

Routing Protocols Overview for Security Devices

- The default route preference value in the "Understanding Route Preference Values" topic for Static and Static LSPs lists the values incorrectly. The correct values are as follows:

How Route Is Learned	Default Preference
Static	5
Static LSPs	6

Security Policy Applications Feature Guide for Security Devices

- On the Overview tab, under IP-Related Predefined Policy Applications, in the topic entitled "Understanding IP-Related Predefined Policy Applications," the Port column for both TCP-ANY and UDP-ANY should indicate 0-65535. The lead-in sentence should read, "Each entry includes the port and a description of the application." TCP-ANY means any application that is using TCP, so there is no default port for it. The same is true for UDP-ANY.

- In the topic entitled "Understanding Miscellaneous Predefined Policy Applications," table "Predefined Miscellaneous Applications" is incomplete. Under the RADIUS row, add a new row:

Table 3: Predefined Miscellaneous Applications

Application	Port	Description
RADIUS Accounting	1813	Enables the collecting of statistical data about users logging in to or out from a LAN and sending the data to a RADIUS Accounting server.

In table "Predefined Miscellaneous Applications" replace the IPsec-NAT row with the following:

Table 4: Predefined Miscellaneous Applications

Application	Port	Description
IKE	500	Internet Key Exchange is the protocol that sets up a security association in the IPsec protocol suite.
IKE-NAT	4500	Helps to perform Layer 3 NAT for S2C IKE traffic.

Application	Port	Description
VoIP	389	Internet Locator Service (ILS)
	522	User Location Service (ULS)
	1503	T.120 Data sharing
	1719	H.225 RAS message
	1720	Q.931 Call Setup
	1731	Audio Call Control
	5060	SIP protocol

Various Guides

- Some Junos OS user, reference, and configuration guides—for example the Junos Software Routing Protocols Configuration Guide, Junos OS CLI User Guide, and Junos OS System Basics Configuration Guide—mistakenly do not indicate SRX Series device support in the "Supported Platforms" list and other related support information; however, many of those documented Junos OS features are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, please refer to Feature Explorer:

  http://pathfinder.juniper.net/feature-explorer/select-software.html?swName=Junos+OS&typ=1.

WLAN Feature Guide for Security Devices

- This guide is missing information that the AX411 Access Point can be managed from SRX100 and SRX110 devices.

- This guide is missing the information that on all branch SRX Series devices, managing AX411 WLAN Access Points through a Layer 3 Aggregated Ethernet (ae) interface is not supported.

Documentation Updates for the Junos OS Hardware Documentation

This section lists outstanding issues with the hardware documentation.

J Series Services Routers Hardware Guide

- The procedure "Installing a DRAM Module" omits the following condition:

  All DRAM modules installed in the router must be the same size (in megabytes), type, and manufacturer. The router might not work properly when DRAM modules of different sizes, types, or manufacturer are installed.

- This guide incorrectly states that only the J2350 Services Router complies with NEBS criteria. It should state that the J2350, J4350, and J6350 routers comply with NEBS criteria.

- This guide is missing information about 100Base-LX connector support for 1-port and 6-port Gigabit Ethernet uPIMs.

SRX Series Services Gateways for the Branch Physical Interface Modules Hardware Guide

- This guide incorrectly documents that slot 3 of the SRX550 Services Gateway can be used to install GPIMs. The correct information is:

  - In Table 10: "SRX Series Services Gateway Interface Port Number Examples", for 2-Port 10 Gigabit Ethernet XPIM, you can install the XPIM only in slot 6 of the SRX550 Services Gateway.

  - In Table 44: "Slots for 20-Gigabit GPIMs, for 20-Gigabit GPIM slots", you can install the GPIM only in slot 6 of the SRX550 Services Gateway.

SRX100 Services Gateway Hardware Guide

- In the "Connecting an SRX100 Services Gateway to the J-Web Interface" section, the following information is missing in the note:

  NOTE: Microsoft Internet Explorer version 6.0 is also supported as backward compatible from Microsoft Internet Explorer version 7.0.

SRX210 Services Gateway Hardware Guide

- In the "Connecting an SRX210 Services Gateway to the J-Web Interface" section, the following information is missing in the note:

  NOTE: Microsoft Internet Explorer version 6.0 is also supported as backward compatible from Microsoft Internet Explorer version 7.0.

- The "SRX210 Services Gateway Specifications" table lists the values for chassis height, chassis width, chassis depth, chassis weight, and noise level incorrectly. The correct values are as follows:

  - Chassis height—1.73 in. (44 mm)

  - Chassis width—11.02 in. (280 mm)

- Chassis depth—7.13 in. (181 mm)

- Chassis weight:

  - 3.46 lb (1.57 kg) for SRX210 Services Gateway without PoE (no interface modules)

  - 3.55 lb (1.61 kg) for SRX210 Services Gateway with PoE (no interface modules)

- Noise level—29.1 dB per EN ISO 7779

SRX220 Services Gateway Hardware Guide

- The "SRX220 Services Gateway Specifications" table lists the values for chassis height, chassis width, chassis depth, chassis weight, and noise level incorrectly. The correct values are as follows:

  - Chassis height—1.73 in. (44 mm)

  - Chassis width—14.29 in. (363 mm)

  - Chassis depth—7.13 in. (181 mm)

  - Chassis weight:

    - 4.52 lb (2.05 kg) for SRX220 models without PoE (no interface modules)

    - 4.62 lb (2.10 kg) for SRX220 models with PoE (no interface modules)

  - Noise level—51.1 dB per EN ISO 7779

SRX240 Services Gateway Hardware Guide

- In the "Connecting the SRX240 Services Gateway to the J-Web Interface" section, the following information is missing in the note:

  > **NOTE:** Microsoft Internet Explorer version 6.0 is also supported as backward compatible from Microsoft Internet Explorer version 7.0.

- The "Maintaining the SRX650 Services Gateway Power Supply" section incorrectly states that the status of the power supplies on the SRX650 Services Gateway can be checked by issuing the **show chassis environment pem** command. The **show chassis environment pem** command is not supported on the SRX650 Services Gateway.

SRX110 Services Gateway 3G USB Modem Quick Start

- The SRX110 Services Gateway 3G USB Modem Quick Start has been updated with the J-Web procedures, and it is available on the Juniper Networks website.

SRX210 Services Gateway 3G ExpressCard Quick Start

- Several tasks are listed in the wrong order. "Task 6: Connect the External Antenna" should appear before "Task 3: Check the 3G ExpressCard Status," because the user needs to connect the antenna before checking the status of the 3G ExpressCard. The correct order of the tasks is as follows:

1. Install the 3G ExpressCard

2. Connect the External Antenna

3. Check the 3G ExpressCard Status

4. Configure the 3G ExpressCard

5. Activate the 3G ExpressCard Options

- In "Task 6: Connect the External Antenna," the following sentence is incorrect and redundant: "The antenna has a magnetic mount, so it must be placed far away from radio frequency noise sources including network components."

- In the "Frequently Asked Questions" section, the answer to the following question contains an inaccurate and redundant statement:

  Q: Is an antenna required? How much does it cost?

  A: The required antenna is packaged with the ExpressCard in the SRX210 Services Gateway 3G ExpressCard kit at no additional charge. The antenna will have a magnetic mount with ceiling and wall mount kits within the package.

  In the answer, the sentence "The antenna will have a magnetic mount with ceiling and wall mount kits within the package" is incorrect and redundant.

SRX210 Services Gateway Quick Start Guide

- The section on installing software packages is missing the following information:

  On SRX210 devices, the **/var** hierarchy is hosted in a separate partition (instead of the *root* partition). If Junos OS installation fails as a result of insufficient space:

  1. Use the **request system storage cleanup** command to delete temporary files.

  2. Delete any user-created files both in the *root* partition and under the **/var** hierarchy.

Related Documentation

- New and Changed Features on page 6
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 24
- Known Issues on page 53
- Resolved Issues on page 57
- Migration, Upgrade, and Downgrade Instructions on page 70

Migration, Upgrade, and Downgrade Instructions

This section includes the following topics:

- Upgrading and Downgrading among Junos OS Releases on page 71
- Upgrading an AppSecure Device on page 72
- Network and Security Manager Support on page 73

- Upgrade and Downgrade Scripts for Address Book Configuration on page 73
- Hardware Requirements on page 75

Upgrading and Downgrading among Junos OS Releases

All Junos OS releases are listed in sequence on the JUNOS Software Dates & Milestones webpage:

http://www.juniper.net/support/eol/junos.html

To help in understanding the examples that are presented in this section, a portion of that table is replicated here. Note that releases footnoted with a 1 are Extended End-of-Life (EEOL) releases.

Product	FRS Date
Junos 12.1	03/28/2012
Junos 11.4[1]	12/21/2011
Junos 11.3	08/15/2011
Junos 11.2	08/03/2011
Junos 11.1	03/29/2011
Junos 10.4[1]	12/08/2010
Junos 10.3	08/15/2010
Junos 10.2	05/28/2010
Junos 10.1	02/15/2010
Junos 10.0[1]	11/04/2009
Junos 9.6	08/06/2009
Junos 9.5	04/14/2009
Junos 9.4	02/11/2009
Junos 9.3[1]	11/14/2008
Junos 9.2	08/12/2008
Junos 9.1	04/28/2008
Junos 9.0	02/15/2008
Junos 8.5[1]	11/16/2007

You can directly upgrade or downgrade between any two Junos OS releases that are within three releases of each other.

- Example: Direct release upgrade

  Release 10.3 → *(bypassing Releases 10.4 and 11.1)* Release 11.2

To upgrade or downgrade between Junos OS releases that are more than three releases apart, you can upgrade or downgrade first to an intermediate release that is within three releases of the desired release, and then upgrade or downgrade from that release to the desired release.

- Example: Multistep release downgrade

  Release 11.3 → *(bypassing Releases 11.2 and 11.1)* Release 10.4 → Release 10.3

Juniper Networks has also provided an even more efficient method of upgrading and downgrading using the Junos OS EEOL releases. EEOL releases generally occur once a calendar year and can be more than three releases apart. For a list of, EEOL releases, go to http://www.juniper.net/support/eol/junos.html

You can directly upgrade or downgrade between any two Junos OS EEOL releases that are within three EEOL releases of each other.

- Example: Direct EEOL release upgrade

  Release 9.3 (EEOL) → *(bypassing Releases 10.0 [EEOL] and 10.4 [EEOL])* Release 11.4 (EEOL)

To upgrade or downgrade between Junos OS EEOL releases that are more than three EEOL releases apart, you can upgrade first to an intermediate EEOL release that is within three EEOL releases of the desired EEOL release, and then upgrade from that EEOL release to the desired EEOL release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 8.5 (EEOL) → *(bypassing Releases 9.3 [EEOL] and 10.0 [EEOL])* Release 10.4 (EEOL) → Release 11.4 (EEOL)

You can even use a Junos OS EEOL release as an intermediate upgrade or downgrade step if your desired release is several releases later than your current release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 9.6 → Release 10.0 (EEOL) → Release 10.2

For additional information about how to upgrade and downgrade, see the *Junos OS Installation and Upgrade Guide*.

Upgrading an AppSecure Device

Use the no-validate Option for AppSecure Devices.

For devices implementing AppSecure services, use the no-validate option when upgrading from Junos OS Release 11.2 or earlier to Junos OS 11.4R1 or later. The application signature package used with AppSecure services in previous releases has been moved from the configuration file to a signature database. This change in location can trigger an error

during the validation step and interrupt the Junos OS upgrade. The no-validate option bypasses this step.

Network and Security Manager Support

Network and Security Manager (NSM) support for SRX Series Services Gateways and J Series Services Routers with Junos OS 12.1X46-D10 is available only with NSM versions 2012.2R6 / 2012.1R10 and later. For additional information, see Network and Security Manager documentation.

Upgrade and Downgrade Scripts for Address Book Configuration

Beginning with Junos OS Release 12.1, you can configure address books under the **[security]** hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the **[security zones]** hierarchy (zone-defined configuration).

You can either define all address books under the **[security]** hierarchy in a zone-attached configuration format or under the **[security zones]** hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see Figure 1 on page 74).

- About Upgrade and Downgrade Scripts on page 73
- Running Upgrade and Downgrade Scripts on page 74
- Upgrade and Downgrade Support Policy for Junos OS Releases on page 75

About Upgrade and Downgrade Scripts

After downloading Junos OS Release 12.1, you have the following options for configuring the address book feature:

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

- **Use the upgrade script**—You can run the upgrade script available on the Juniper Networks support site to configure address books using the new zone-attached configuration format. When upgrading, the system uses the zone names to create address books. For example, addresses in the trust zone are created in an address book named **trust-address-book** and are attached to the trust zone. IP prefixes used in NAT rules remain unaffected.

  After upgrading to the zone-attached address book configuration:

  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.

  - You cannot configure address books using the J-Web interface.

For information on how to configure zone-attached address books, see the Junos OS Release 12.1 documentation.

- **Use the downgrade script**—After upgrading to the zone-attached configuration, if you want to revert to the zone-defined configuration, use the downgrade script available on the Juniper Networks support site. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

NOTE: Before running the downgrade script, make sure to revert any configuration that uses addresses from the global address book.

Figure 1: Upgrade and Downgrade Scripts for Address Books

Download Junos OS
Release 11.2 or later.

zone-defined
address book

Run the upgrade script.

zone-attached
address book
configuration

- Global address book is available by default.
- Address book is defined under the security hierarchy.
- Zones need to be attached to address books.

Run the downgrade script.

Note: Make sure to revert any configuration that uses addresses from the global address book.

g030699

Running Upgrade and Downgrade Scripts

The following restrictions apply to the address book upgrade and downgrade scripts:

- The scripts cannot run unless the configuration on your system has been committed. Thus, if the zone-defined address book and zone-attached address book configurations are present on your system at the same time, the scripts will not run.

- The scripts cannot run when the global address book exists on your system.

- If you upgrade your device to Junos OS Release 12.1 and configure logical systems, the master logical system retains any previously configured zone-defined address book configuration. The master administrator can run the address book upgrade script to

convert the existing zone-defined configuration to the zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems.

> *i*   NOTE: **You cannot run the downgrade script on logical systems.**

For information about implementing and executing Junos operation scripts, see the *Junos OS Configuration and Operations Automation Guide*.

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see http://www.juniper.net/support/eol/junos.html .

Hardware Requirements

Transceiver Compatibility for SRX Series and J Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on SRX Series and J Series interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport SFP interface modules as long as they are provided by Juniper Networks. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

Power and Heat Dissipation Requirements for J Series PIMs

On J Series Services Routers, the system monitors the PIMs and verifies that the PIMs fall within the power and heat dissipation capacity of the chassis. If power management is enabled and the capacity is exceeded, the system prevents one or more of the PIMs from becoming active.

> ⚠ CAUTION: Disabling the power management can result in hardware damage if you overload the chassis capacities.

You can also use CLI commands to choose which PIMs are disabled. For details about calculating the power and heat dissipation capacity of each PIM and for troubleshooting procedures, see the *J Series Services Routers Hardware Guide*.

Supported Third-Party Hardware

The following third-party hardware is supported for use with J Series Services Routers running Junos OS.

- **USB Modem**

  We recommend using a U.S. Robotics USB 56K V.92 Modem, model number USR 5637.

- **Storage Devices**

  The USB slots on J Series Services Routers accept a USB storage device or USB storage device adapter with a CompactFlash card installed, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the USB device is installed and configured, it automatically acts as a secondary boot device if the primary CompactFlash card fails on startup. Depending on the size of the USB storage device, you can also configure it to receive any core files generated during a router failure. The USB device must have a storage capacity of at least 256 MB.

  Table 5 on page 76 lists the USB and CompactFlash card devices supported for use with the J Series Services Routers.

Table 5: Supported Storage Devices on the J Series Services Routers

Manufacturer	Storage Capacity	Third-Party Part Number
SanDisk—Cruzer Mini 2.0	256 MB	SDCZ2-256-A10
SanDisk	512 MB	SDCZ3-512-A10
SanDisk	1024 MB	SDCZ7-1024-A10
Kingston	512 MB	DTI/512KR
Kingston	1024 MB	DTI/1GBKR
SanDisk—ImageMate USB 2.0 Reader/Writer for CompactFlash Type I and II	N/A	SDDR-91-A15
SanDisk CompactFlash	512 MB	SDCFB-512-455
SanDisk CompactFlash	1 GB	SDCFB-1000.A10

J Series CompactFlash and Memory Requirements

Table 6 on page 77 lists the CompactFlash card and DRAM requirements for J Series Services Routers.

Table 6: J Series CompactFlash Card and DRAM Requirements

Model	Minimum CompactFlash Card Required	Minimum DRAM Required	Maximum DRAM Supported
J2320	1 GB	1 GB	1 GB
J2350	1 GB	1 GB	1 GB
J4350	1 GB	1 GB	2 GB
J6350	1 GB	1 GB	2 GB

Related Documentation

- New and Changed Features on page 6
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 24
- Known Issues on page 53
- Resolved Issues on page 57
- Documentation Updates on page 63

Junos OS Release Notes for High-End SRX Series

Powered by Junos OS, Juniper Networks high-end SRX Series Services Gateways provide robust networking and security services. High-end SRX Series Services Gateways are designed to secure enterprise infrastructure, data centers, and server farms. The high-end SRX Series Services Gateways include the SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices.

New and Changed Features

The following features have been added to Junos OS Release 12.1X46-D10. Following the description is the title of the manual or manuals to consult for further information.

> NOTE: For the latest updates about support and issues on Junos Pulse, see the Junos Pulse Release Notes.

Software Features

Application Layer Gateways (ALGs)

- **ALG message buffer optimization**—Starting in Junos OS Release 12.1X46-D10, the ALG message buffer optimization feature is enhanced to reduce high memory consumption. This feature is supported on all SRX Series and J Series devices.

  A message buffer is allocated only when the packet is ready to process. The buffer is freed after the packet completes ALG handling, including modifying the payload, performing NAT, opening a pinhole for a new connection between a client and a server, and transferring data between a client and a server located on opposite sides of a Juniper Networks device.

  This feature has the following enhancements:

  - Unnecessary objcache buffering is avoided, resulting in low memory utilization.
  - jbuf manipulation is used to simplify the message buffer logic.
  - Full-fledged message buffer support for ALG line breaker is more flexible.
  - ALG Manager and ALG plug-in logic clarity are optimized.

[See alg-manager.]

- **IPv6 support for PPTP ALG**—Starting with Junos OS Release 12.X46, this feature is supported on all SRX Series devices.

  PPTP ALG provides an ALG for the Point-to-Point Tunneling Protocol (PPTP). The PPTP is a Layer 2 protocol that tunnels PPP data across TCP/IP networks. The PPTP client is freely available on Windows systems and popularly applied on Linux systems; it is widely deployed for building VPNs.

  To support IPv6, the PPTP ALG parses both IPv4 and IPv6 PPTP packets, performs NAT, and then opens a pinhole for the data tunnel. The flow module supports IPv6 to parse the GRE packet and use the GRE call ID as fake port information to search the session table and gate table.

  [See PPTP ALG Feature Guide for Security Devices.]

- **IPv6 support for RTSP ALG**—This feature is supported on all SRX Series and J Series devices.

  RTSP (Real-Time Streaming Protocol) is an Application Layer protocol for controlling the delivery of data with real-time properties. The RTSP ALG accesses existing media files over the network and controls the replay of the media.

  Starting with Junos OS Release 12.1X46-D10, IPv6 is supported on the RTSP ALG along with NAT-PT mode and NAT64 address translation.

  This feature enables the RTSP ALG to parse IPv6 RTSP packets, open an IPv6 pattern pinhole, and translate the Layer 7 IPv6 address according to the NAT configuration. Also, support for IPv6 RTSP transaction pass through under permission policy and IPv6 RTSP transaction pass through under NAT-PT and NAT 64 are enabled.

  [See SIP RTSP ALG Feature Guide for Security Devices.]

- **IPv6 support for SIP ALG**—This feature is supported on all SRX Series and J Series devices.

  Starting with Junos OS Release 12.1X46-D10, IPv6 is supported on the SIP ALG along with NAT-PT mode and NAT64 address translation.

  The SIP ALG processes the IPv6 address in the same way it processes the IPv4 address for updating the payload if NAT is configured and opening pinholes for future traffic.

  NAT-PT is implemented by normal NAT from IPv6 address to IPv4 address and vice versa. The SIP ALG processes those address translation in payload just as the addresses are processed in normal NAT.

  NAT64 is a mechanism to allow IPv6 hosts to communicate with IPv4 servers. NAT64 is required to keep the IPv6 to IPv4 address mapping.

  Previously Session Traversal Utilities for NAT (STUN) worked without the SIP ALG. This means that the SIP ALG was not involved when persistent NAT was configured.

  Starting with Junos OS Release 12.1X46-D10, STUN can coexist with the SIP ALG and SIP ALG is involved when persistent NAT is configured.

  [See SIP ALG Feature Guide for Security Devices.]

Chassis Cluster

- Chassis cluster—Starting in Junos OS Release 12.1X46-D10, the SRX5K-MPC adds the support of using 40-Gigabit Ethernet and 100-Gigabit Ethernet ports as chassis cluster fabric ports. This feature is supported on the SRX5400, SRX5600, and SRX5800. This enhancement saves one more slot on chassis and also improves chassis cluster fabric link performance. In addition, you can also use 10G port on SRX5K-MPC as fabric port with a 10x10GE MIC installed on it.

  [See Understanding Chassis Cluster Fabric Links.]

Dynamic Host Configuration Protocol (DHCP)

- **DHCP relay**—Starting in Junos OS Release 12.1X46-D10, this feature is supported on all high-end SRX Series devices.

  The existing DHCP relay feature has been enhanced to include support for high-end SRX Series devices along with chassis cluster support.

  You can configure DHCP relay options on the device and enable the device to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

  To configure the DHCP relay agent on the device, include the **dhcp-relay** statement at the [**edit forwarding-options**] hierarchy level.

  [See Understanding DHCP Relay Agent Operation.]

Flow and Processing

- **Enhanced IPv6 support for the screen feature**—This feature is supported on all high-end SRX Series devices.

  IPv6 support is extended for the following screen features:

  - IPv6 extension header checking and filtering

  - IPv6 packet header checking and filtering

  - ICMPv6 checking and filtering

  New statements and commands allow you to configure these enhancements using security zones similar to previous screen configurations. You can enable, disable, and update screens to drop packets, create logs, and provide increased statistics for IPv6 traffic.

  > NOTE: By default, IPv6 packets bypass the screen feature.

  [See Understanding IPv6 Support for Screens.]

- **Enhancements to flow trace options**—This feature is supported on all high-end SRX Series devices.

  Starting in Junos OS Release 12.1X46-D10, flow trace granularity has been enhanced to filter logs effectively. As a result you can access relevant trace messages easily and

avoid large traces that slow down your system. You can set the level of message you want displayed by using the new **trace-level** statement at the **[edit security flow traceoptions]** hierarchy level. And, use new flags to trace additional operations such as fragmentation, high availability, multicast, session, tunnel, and route.

[See traceoptions (Security Flow).]

- **Monitoring flow sessions**—This feature is supported on all high-end SRX Series devices.

  Beginning with Junos OS Release 12.1X46-D10, you can monitor flow using filters that match different criteria (such as source and destination addresses). New operational mode commands **monitor security flow filter** and **monitor security flow file** have been added. These commands allow you to debug without having to commit or modify your running configuration. Previously, you were required to commit the configuration to turn on trace options, which could possibly change the state of your device.

  [See Monitoring Security Flow Sessions Overview.]

General Packet Radio Service (GPRS)

- **NAT for GPRS tunneling protocol (GTP):**—Starting in Junos OS Release 12.1X46-D10, static NAT for GTP packets is supported on all high-end SRX Series devices.

  This feature has the following enhancements:

  - For GTP, control (GTP-C), as part of the GPRS IP address negotiation, embedded IP addresses are included in the packet data protocol (PDP) context request or response messages.

  - For GTP, user plane (GTP-U), GTP-U carries encapsulated user payload in an IP packet. When NAT is enabled, only the outer IP packet needs to be translated, the embedded IP addresses will not be translated.

  [See Understanding GTP-U Inspection.]

- **GTP unified in-service software upgrade support (ISSU)**—Junos OS Release 12.1X46-D10 adds support for unified ISSU on the GPRS tunneling protocol (GTP). This feature is supported on all high-end SRX Series devices.

  GTP supports unified ISSU between two SRX Series devices running two different Junos OS releases. Unified ISSU is applied on a chassis cluster, enabling a software upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic.

[See Understanding GTP-U Inspection.]

Interfaces and Routing

- **Link aggregation**—Starting in Junos OS Release 12.1X46-D10, the SRX5K-MPC supports the LAG and LACP features on the SRX5400, SRX5600, and SRX5800.

The following LAG and LACP features are supported:

- Increases bandwidth, provides graceful degradation as failure occurs, and increases availability.

- Provides network redundancy by load-balancing traffic across all available links. If one of the links should fail, the system automatically load-balances traffic across all remaining links.

- Enables automatic addition and deletion of individual links to the aggregate bundle without user intervention.

- Provides link monitoring to check whether both ends of the bundle are connected to the correct group, enables or disables link protection, configures the LACP interval, and supports centralized and distributed modes.

[See LAG and LACP Support on the SRX5000 Module Port Concentrator.]

[See Understanding Aggregated Ethernet Interfaces.]

IPsec VPN

- **Dead peer detection (DPD) enhancements**—This feature is supported on all SRX Series devices.

  Network devices use the DPD protocol to verify the existence and availability of other peer devices. The default DPD mode **optimized** sends probes if there is no incoming IKE or IPsec traffic from the peer within a configured interval after outgoing packets are sent to the peer. The **always-send** option sends DPD probes at configured intervals regardless of traffic activity between peers. A new configuration option **probe-idle-tunnel** at the [**edit security ike gateway dead-peer-detection**] hierarchy level sends DPD probes when there is no incoming or outgoing IKE or IPsec traffic between peers.

  > NOTE: We recommend that you configure **probe-idle-tunnel** instead of **always-send**.

  For all DPD modes, Phase 1 and Phase 2 security associations are cleared if a specified number of probes are sent with no response from the peer.

  [See Understanding Dead Peer Detection.]

- **IPsec VPN performance enhancements**—Starting in Junos OS Release 12.1X46-D10, a new configuration statement, **ipsec-performance-acceleration**, has been introduced under the [**edit security flow**] hierarchy to enable IPsec VPN performance acceleration. This feature is supported on SRX3400, SRX3600, SRX5600, and SRX5800 devices.

  By default, VPN performance acceleration is disabled on SRX Series devices. Enabling VPN performance acceleration can improve VPN throughput under certain conditions.

  The following functions are not supported:

  - VPN traffic ACL accounting on physical egress and ingress interface

  - VPN traffic physical interface filter-based policer

- VPN traffic physical interface QoS feature (classifier, remarking, scheduling, and shaping)

- **Multiple traffic selectors on a route-based VPN**—This feature is supported on all SRX Series devices.

  A traffic selector (also known as a proxy ID in IKEv1) is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. With this feature, you can define multiple traffic selectors within a specific route-based VPN, resulting in a unique SA for each traffic selector configured. Only traffic that conforms to a traffic selector is permitted through the associated IPsec SA.

  To configure a traffic selector, use the **traffic-selector** configuration statement at the [**edit security ipsec vpn** *vpn-name*] hierarchy level. The traffic selector pair is defined with the mandatory **local-ip** *ip-address* and **remote-ip** *ip-address* statements. The CLI operational command **show security ipsec security-association traffic-selector** *traffic-selector* displays SA information for the specified traffic selector.

  [See Understanding Traffic Selectors in Route-Based VPNs.]

- **Support for IPv6 address encapsulation in route-based one-to-one site-to-site VPN tunnels**—This feature is supported on all SRX Series devices.

  In tunnel mode, IPsec encapsulates the original IP datagram—including the original IP header—within a second IP datagram. The outer IP header contains the IP address of the gateway, while the inner header contains the ultimate source and destination IP addresses. The outer and inner IP headers can have a protocol field of IPv4 or IPv6. As of Junos OS Release 12.1X46-D10, the following tunnel modes are supported on SRX Series devices:

  - IPv4-in-IPv4 tunnels encapsulate IPv4 packets inside IPv4 packets.

  - IPv6-in-IPv6 tunnels encapsulate IPv6 packets inside IPv6 packets.

  - IPv6-in-IPv4 tunnels encapsulate IPv6 packets inside IPv4 packets.

  - IPv4-in-IPv6 tunnels encapsulate IPv4 packets inside IPv6 packets.

  There are no new CLI configuration statements for this feature.

  IPv4 and IPv6 traffic can be routed into a single IPv4 or IPv6 tunnel; the st0 interface bound to the tunnel must be configured for both family inet and family inet6. Dual stack tunnels—parallel IPv4 and IPv6 tunnels over a single physical external interface to different VPN peers—are also supported.

  [See VPN Feature Support for IPv6 Addresses.]

- **IKEv2 configuration payload support with RADIUS**—This feature is supported on all SRX Series devices.

  Configuration payload is an Internet Key Exchange (IKE) version 2 feature used to propagate provisioning information from an IKE responder to the IKE initiator. Starting with Junos OS Release 12.1X46-D10, IKEv2 configuration payload is supported with route-based VPNs only. The following attribute types, defined in RFC 5996, *Internet*

Key Exchange Protocol Version 2 (IKEv2), can be returned to the IKE initiator by the IKE responder:

- INTERNAL_IP4_ADDRESS

- INTERNAL_IP4_NETMASK

- INTERNAL_IP4_DNS

For the IKE responder to provide the initiator with provisioning information, it must acquire the information from a specified source such as a RADIUS server. Provisioning information can also be returned from a DHCP server through a RADIUS server. On the RADIUS server, the user information should not include an authentication password. As in previous Junos OS releases for the SRX Series, the RADIUS server profile is bound to the IKE gateway using the **xauth access-profile** *profile-name* configuration at the [**edit security ike gateway** *gateway-name*] hierarchy level.

This feature is supported only for point-to-multipoint secure tunnel (st0) interfaces. For point-to-multipoint interfaces, the interfaces must be numbered and the addresses in the configuration payload INTERNAL_IP4_ADDRESS attribute type must be within the subnetwork range of the associated point-to-multipoint interface.

> **NOTE:** IKEv2 on SRX Series devices does not support policy-based VPNs or VPN monitoring.

[See Understanding Internet Key Exchange Version 2.]

- **IKEv2 with NAT-T and dynamic endpoint VPN**—This feature is supported on all SRX Series devices.

  Starting with Junos OS 12.1X46-D10, both IKEv2 initiators and responders in a route-based VPN can be behind NAT devices. The IKEv2 NAT-T feature supports IPsec traffic that crosses NAT devices. Static NAT and dynamic NAT are supported. In static NAT, there is a one-to-one relationship between the private and the public addresses. In dynamic NAT, there is a many-to-one or many-to-many relationship between the private and public addresses.

  Dynamic endpoint (DEP) VPN is a Junos OS feature that covers IKEv2 initiator and responder perspectives. From the initiator's perspective, DEP VPN covers the situation where the IKE external interface address is not fixed and is therefore not known by the responder. This situation can occur when the peer's address is dynamically assigned by an ISP or when the peer's connection crosses a NAT device that allocates addresses from a dynamic address pool. From the responder's perspective, DEP VPN describes either a finite number of VPNs that are created for a number of VPN peers in a many-to-many scenario or a shared VPN in a many-to-one scenario.

  Starting with Junos OS 12.1X46-D10, the default value for the **nat-keepalive** option configured at the [**edit security ike gateway** *gateway-name*] hierarchy level has been changed from 5 seconds to 20 seconds.

  [See Understanding NAT-T.]

IP Spoofing

- **IP spoofing in transparent mode**—Starting in Junos OS Release 12.1X46-D10, this feature is supported on all high-end SRX Series devices.

  The IP spoofing feature has been enhanced to include Layer 2 transparent mode support. IP spoofing is most frequently used in denial-of-service attacks. In an IP spoofing attack, the attacker gains access to a restricted area of the network and inserts a false source address in the packet header to make the packet appear to come from a trusted source. When SRX Series devices are operating in transparent mode, the IP spoof-checking mechanism makes use of address book entries.

  > **NOTE:** IP spoofing in Layer 2 transparent mode does not support DNS and wildcard addresses.

  [See Understanding IP Spoofing in Layer 2 Transparent Mode.]

J-Web

- **Management support for NAT options**—Starting in Junos OS Release 12.1X46-D10, support is provided to monitor the following NAT options on all SRX Series devices:

  - Utilization for all source pools

  - Successful, failed, and current sessions for source pools, source rules, destination rules, and static rules

  - Source addresses and source ports for static rules

  - Source ports for source rules

- Support is provided to configure the following NAT options on all SRX Series devices:

  - Source address and port as match criteria for static rules

  - Source port as match criteria for source rules

  - Upper and lower thresholds at which an SNMP trap is triggered for source rules and pools, destination rules, and static rules

- **User Firewall J-Web support**

  - **Source identity-based firewall policy**—Starting in Junos OS Release 12.1X46-D10, this feature is supported on the existing Firewall Policies Configuration and Monitoring Policies pages on all high-end SRX Series devices. This feature allows you to configure and monitor source identities in a firewall policy.

  - **Configure firewall authentication integrated with user firewall**—Starting in Junos OS Release 12.1X46-D10, this feature is supported on all high-end SRX Series devices. You use this feature by specifying the access profile and SSL termination profile.

  - **New J-Web pages for user firewall**—Starting in Junos OS Release 12.1X46-D10, new user firewall pages are supported on all high-end SRX Series devices.

The following webpages have been added to the J-Web user interface:

- **Authentication Priority Configuration Page**—You can either disable an optional authentication source or reassign a unique priority to it.

- **Local Authentication Configuration Page and Local Authentication Monitoring Page**—You can configure and monitor local Firewall authentication.

- **UAC Settings Configuration Page and UAC Authentication Monitoring Page**—You can configure UAC and monitor UAC authentication.

- **Allow adding a new policy and moving an existing policy to an arbitrary location**

  - **Firewall Policies Configuration Page Options**—Starting in Junos OS Release 12.1X46-D10, several new options on the Firewall Policies Configuration page are supported on high-end SRX Series devices. The Add menu includes Add before and Add after options that allow you to add a new policy before or after a selected policy. On the Move menu, there is a new Move to option that allows you to specify a target location. You can also drag and drop a policy to the target location.

  - **Checking Policies Monitoring Page**—Starting in Junos OS Release 12.1X46-D10, the Move to option on the Checking Policies Monitoring page is supported on high-end SRX Series devices.

Management Information Bases (MIBs)

- **SNMP aggregation for policy MIBs**—Starting in Junos OS Release 12.1X46-D10, this feature is supported on all SRX Series devices.

  A set of systemwide policy statistics such as policy-allowed packets, bytes and rates, policy-dropped packets, bytes and rates, and policy flows allowed and rate statistics have been added in the enterprise-specific policy MIB JUNIPER-JS-POLICY-MIB. You can obtain the policy statistics by using the SNMP agent or the CLI operational mode commands. Use the following CLI commands to set, clear, and display the systemwide policy statistics:

  - **set security policies policy-stats system-wide <disable | enable>**—Configures systemwide policy statistics. Disabled by default.

  - **clear security policies statistics**—Clears the systemwide policy statistics.

  - **show snmp mib walk jnxJsPolicySystemStats**—Displays both IPv4 and IPv6 statistics.

  - **show snmp mib walk jnxJsPolicySystemStatsIPv4**—Displays only IPv4 statistics.

  [See Policy Objects MIB.]

Modular Interface Cards

SRX5600 and SRX5800 Services Gateway MPC Software Features—The SRX5K-MPC is a Modular Port Concentrator (MPC) that is supported on the SRX5400, SRX5600, and SRX5800.

The following features are supported on the SRX5K-MPC:

- Load balancing among SPUs using hash-based forwarding

  > **NOTE:** When the SRX5K-MPC is installed on SRX5600 and SRX5800 devices, the default session distribution mode is set to hash-based distribution mode on the devices. The hash-based distribution mode is the only mode supported on the SRX5K-MPC.

- Filtering support

- Filter-based forwarding at logical interfaces of revenue ports, firewall filter applied at loopback interface of chassis, policer applied at loopback interface of chassis

- Interface ingress policing

- Following types of threshold-based flood protection:

  - UDP-based flood protection

  - ICMP-based flood protection

  - TCP source-based SYN flood protection

  - TCP destination-based SYN flood protection

Screen

- Screen features—Starting in Junos OS Release 12.1X46-D10, the SRX5K-MPC supports screen features on the SRx5400, SRX5600, and SRX5800.

  The following screen options are supported:

  - Statistics-based screens

  - Signature-based screens

  [See Understanding Screen Options on the SRX5000 Module Port Concentrator.]

  [See Denial-of-Service Attacks Feature Guide for Security Devices.]

Stream Control Transmission Protocol (SCTP)

- **SCTP payload protocol blocking**—Starting in Junos OS Release 12.1X46-D10, the **permit** traffic configuration is added to allow all types of payload protocol traffic. This feature is supported on all high-end SRX Series devices. This feature has the following enhancements:

  - The default behavior for SCTP payload protocol traffic was permit all. Now, the default behavior is drop all. However, the behavior can be changed to permit all by configuration.

  - The payload protocol traffic can be permitted by configuring the decimal value of the SCTP protocol identifiers or the name in the permit list.

- The payload protocol traffic can be dropped by configuring the decimal value of the SCTP protocol identifiers or the name in the drop list.

[See Understanding Stream Control Transmission Protocol.]

- **Support for SCCP v20**—This feature is supported on all SRX Series devices.

Starting in Junos OS Release 12.1X46-D10, the SCCP ALG supports version 20. In SCCP v20, several SCCP messages have been updated with a new format.

[See Understanding SCCP ALGs.]

[See *Understanding SCCP ALGs*.]

- **SCTP rate limiting**—Starting in Junos OS Release 12.1X46-D10, the rate limiting functionality is extended with a generalized SCTP payload protocol rate limiting function. This feature is supported on all high-end SRX Series devices. This feature has the following enhancements:

  - The rate limiting function supports decimal identifier values for Internet Assigned Numbers Authority (IANA) SCTP protocols and synonyms for the well-known IANA SCTP protocols.

  - Each profile can be configured with many IP addresses. Each IP address can be configured with many protocols.

[See Understanding Stream Control Transmission Protocol.]

Unified Threat Management (UTM)

- **UTM antivirus, antispam, and content filtering support**—Starting in Junos OS Release 12.1X46-D10, Sophos antivirus, antispam, and content filtering features are supported on all SRX Series devices.

The existing CLI operational commands **show security utm anti-virus status** and **show security utm anti-virus statistics** have been enhanced to display the aggregated status and statistics from all Flexible PIC Concentrators (FPCs) and PICs. You can use the following new operational commands to display the status and statistics of each FPC and PIC:

  - **show security utm anti-virus status fpc**

  - **show security utm anti-virus status fpc fpc-slot** *fpc-slot* **pic-slot** *pic-slot*

  - **show security utm anti-virus statistics fpc**

  - **show security utm anti-virus statistics fpc fpc-slot** *fpc-slot* **pic-slot** *pic-slot*

[See show security utm anti-virus status.]

[See show security utm anti-virus statistics.]

- **UTM Web filtering support**—Starting in Junos OS Release 12.1X46-D10, the enhanced Web filtering feature is supported on all SRX Series devices.

The existing CLI operational commands **show security utm web-filtering status** and **show security utm web-filtering statistics** have been enhanced to display the aggregated status and statistics from all Flexible PIC Concentrators (FPCs) and PICs. You can use

the following new operational commands to display the status and statistics of each FPC and PIC:

- **show security utm web-filtering status fpc**

- **show security utm web-filtering status fpc fpc-slot** *fpc-slot* **pic-slot** *pic-slot*

- **show security utm web-filtering statistics fpc**

- **show security utm web-filtering statistics fpc fpc-slot** *fpc-slot* **pic-slot** *pic-slot*

[See show security utm web-filtering status.]

[See show security utm anti-virus statistics]

Virtual Private Networks (VPNs)

- **Enhanced X2 interface monitoring**—This feature is supported on all SRX Series devices.

  In an LTE mobile network, X2 interfaces are used to connect Evolved Node Bs (eNodeBs) for signal handover, monitoring, and radio coverage. SRX Series devices connect these eNodeBs using IPsec tunnels.

  This feature enables you to monitor traffic between eNodeBs by snooping into the clear text traffic as it flows from one IPsec tunnel to another. Use the **monitor-filter** statement at the **[edit security forwarding-options]** hierarchy level to duplicate clear text packets and send them to the physical interface. You can then use Ethereal or other packet analyzers to verify or collect the X2 traffic.

  [See Understanding X2 Traffic Monitoring .]

Web Authentication

- **Web-redirect firewall authentication**—Starting in Junos OS Release 12.1X46-D10, Web authentication redirect enhancement is provided on all SRX Series devices.

  With this feature, when you attempt to initiate a connection across the firewall, after successful authentication the browser launches your original destination URL without your needing to retype the URL.

  The following message is displayed:

  ```
  Redirecting to the original url, please wait
  ```

 [See Firewall User Authentication Overview]

Hardware Features

SRX5400 Services Gateway

- The SRX5400 Services Gateway (see) expands the SRX Series family of next-generation security platforms, delivering a high-performance, highly scalable, carrier-class security device with multiprocessor architecture. The SRX5400 Services Gateway is 5 rack units (U) tall. You can stack eight services gateways in a rack that is at least 48 U (89.3 in. or 2.24 m) in height if it has a 1 in. cap between for increased port density per unit of floor space. The services gateway provides four slots that you can populate with one Switch Control Board (SCB) and up to three additional cards comprised of an SPC and MPCs.

> **NOTE:** The SRX5400 Services Gateway supports only the SPC II (SRX5K-SPC-4-15-320) and does not support the SRX5K-SPC-2-10-40 SPC.

Figure 2: SRX5400 Services Gateway Front Panel
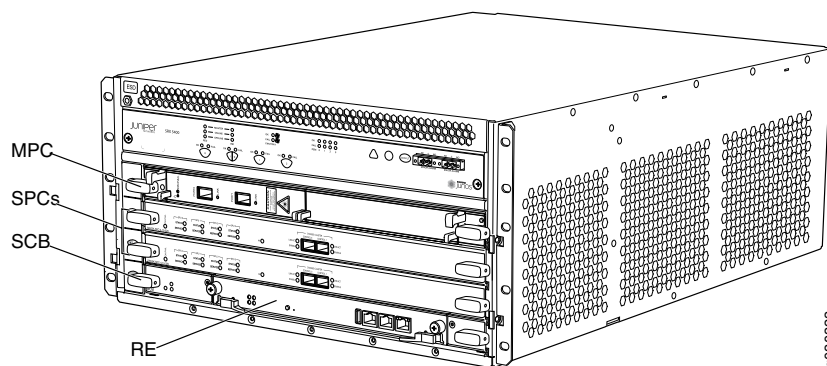
> **NOTE:** The SRX5400 Services Gateway only supports the SRX5K-MPC, and does not support older SRX5000 Series I/O cards (IOCs) or Flex IOCs cards such as:
>
> - SRX5K-40GE-SFP
>
> - SRX5K-4XGE-XFP
>
> - SRX5K-FPC-IOC

> **NOTE:** The SRX5400 Services Gateway supports Junos OS 12.1x46-D10 and later versions. It does not support previous Junos OS versions.

[See Firewall SRX5400 Services Gateway Hardware Guide.]
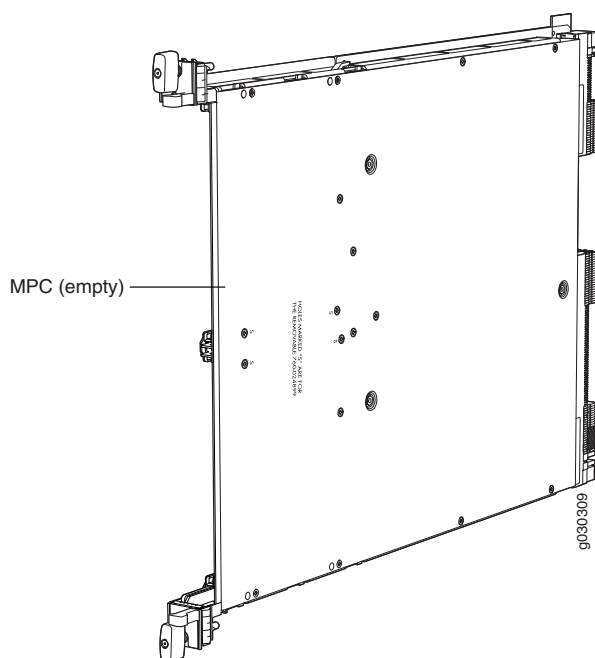
SRX5K-MPC IOC for the SRX5000 Line of Services Gateways

The SRX5K-MPC (see Figure 3 on page 91) is an interface card with two slots that accept MICs which add Ethernet ports to your services gateway. An MPC with MICs installed functions in the same way as a regular IOC but allows you to add different types of Ethernet ports to your device. You can add just one MIC; or you can add two MICs of the same or different types.

> NOTE: The SRX5K-MPC card is supported on the SRX5400, SRX5600, and SRX5800 Services Gateways. The SRX5400 Services Gateway supports only MPCs. It does not support legacy cards such as IOCs or Flex IOCs.

Figure 3: SRX5K-MPC

[See Modular Port Concentrator SRX5K-MPC.]

MICs for the SRX5000 Line of Services Gateways

You use MICs and MPCs to add different combinations of Ethernet interfaces to your services gateway to suit the specific needs of your network. The following three new MICs are supported on the SRX5000 line of services gateways:

SRX-MIC-1X100G-CFP

The SRX-MIC-1X100G-CFP (see Figure 4 on page 92) can be installed in an MPC to add one 100-Gigabit Ethernet CFP port.

Figure 4: SRX-MIC-1X100G-CFP
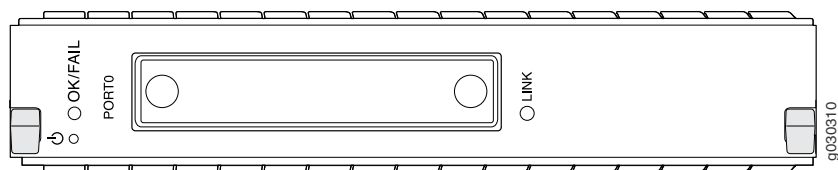
[See SRX-MIC-1X100G-CFP.]

SRX-MIC-2X40G-QSFP

The SRX-MIC-2X40G-QSFP (see Figure 5 on page 92) can be installed in an MPC to add two 40-Gigabit quad small form-factor pluggable (QSFP) Ethernet ports.

Figure 5: SRX-MIC-2X40G QSFP
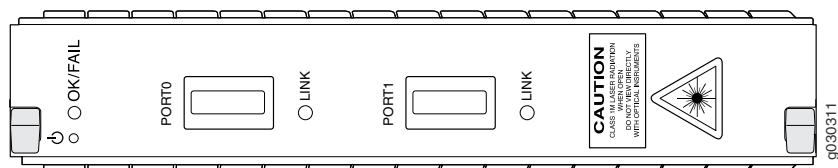
[See SRX-MIC-2X40G-QSFP.]

SRX-MIC-10XG-SFPP

The SRX-MIC-10XG-SFPP (see Figure 6 on page 92) can be installed in an MPC to add ten 10-Gigabit Ethernet SFP+ ports.

Figure 6: SRX-MIC-10XG SFPP
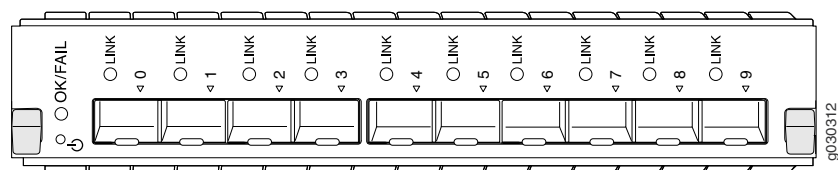
[See SRX-MIC-10XG-SFPP.]

Related Documentation

- Known Issues on page 121
- Resolved Issues on page 126
- Documentation Updates on page 134
- Changes in Behavior and Syntax on page 92
- Known Behavior on page 102

Changes in Behavior and Syntax

The following current system behavior, configuration statement usage, and operational mode command usage might not yet be documented in the Junos OS documentation:

Application Firewall

- Prior to Junos OS Release 11.4R6, when a rule specifies **dynamic-application junos:HTTP** without specifying any other nested application, the rule matches all HTTP traffic whether the traffic contains a nested application or not.

  In Junos OS Release 11.4R6 and later, that functionality has changed. When a rule specifies **dynamic-application junos:HTTP**, only HTTP traffic with no nested members is matched.

  Consider the following application firewall ruleset:

  ```
  rule-sets http-ruleset {
    rule rule1 {
      match {
        dynamic-application [junos:HTTP];
      }
      then {
        deny;
      }
    }
    default-rule {
      permit;
    }
  }
  ```

  Prior to Junos OS Release 11.4R6, the sample rules would be applied to traffic as shown in the following list:

  - HTTP traffic with or without nested applications would be denied by rule1.

    HTTP traffic with a nested application, such as junos:FACEBOOK or junos:TWITTER, would be denied by rule1.

  - All other traffic would be permitted by the default rule.

  In Junos OS Release 11.4R6 and later, the dynamic application junos:HTTP matches only the HTTP traffic that contains no recognizable nested application. The sample rules would now be applied differently:

  - Only the HTTP traffic with no nested application would be denied by rule1.

    HTTP traffic with a nested application, such as junos:FACEBOOK or junos:TWITTER, would no longer match rule1.

  - All other traffic would be permitted by the default rule.

    HTTP traffic with a nested application, such as junos:FACEBOOK or junos:TWITTER, would be permitted by the default rule.

- In Junos OS Release 12.1X46-D10 and earlier, if a nested application is not configured in any rule, then the nested application would match the default rule and take action specified in the default rule.

  Starting in Junos OS Release 12.1X46-D10, the functionality has changed. If a nested application matches the default rule, then the application firewall uses the application type to match the rule and takes action specified in the rule. Use the **set security**

application-firewall nested-application dynamic-lookup enable command to control the behavior of the nested application, so that both the application and the nested application are consistent.

The default behavior of nested application before Junos OS Release 12.1X46-D10:

- Application firewall matches with the specific rule, if the nested application is configured explicitly in a rule.

- Application firewall matches with the default rule, if the nested application is not configured explicitly in a rule.

- Records the statistics of the application firewall in the matched rule.

The new behavior of nested application in Junos OS Release 12.1X46-D10:

- Application firewall matches with an application rule during application firewall policy lookup, if there is no explicit rule for the nested application.

- Application firewall matches with a specific rule, if the nested application is configured explicitly in a rule.

- Records the statistics of the application firewall in the matched rule.

Application-Level Distributed Denial of Service

- Application-level distributed denial of service, which is used to identify malicious bot clients and to drop or deny traffic if requests exceed configured thresholds, will be deprecated in future releases. As a replacement product for this feature, we recommend that you migrate to the Juniper DDoS Secure product line. For more details, contact your sales engineer.

Command-Line Interface (CLI)

New or Changed CLI

- On all high-end SRX Series devices, on SPC and next-generation SPCs, IDP dedicated modes are supported only with the **inline-tap** option. In the inline-tap mode option, the **weight equal** option is not supported.

Other IDP dedicated mode configurations such as dedicated weight IDP, dedicated firewall, and dedicated equal are not supported.

The following IDP dedicated mode configuration statements are not supported:

- **set security forwarding-process application-services maximize-idp-sessions weight firewall**

- **set security forwarding-process application-services maximize-idp-sessions weight idp**

- set security forwarding-process application-services maximize-idp-sessions weight equal

- set security forwarding-process application-services maximize-idp-sessions inline-tap weight equal

- The following configuration statements are supported:

  - set security forwarding-process application-services maximize-idp-sessions inline-tap weight firewall

  - set security forwarding-process application-services maximize-idp-sessions inline-tap weight idp

- Starting in Junos OS Release 12.1X46-D10, on SRX3400 and SRX3600 devices, the value for licenses used in the output of the **show system license** command correctly displays a 1 in the full-cp-key field. Prior to this release, the output displayed a 0.

- Prior to Junos OS Release 12.1X46-D10, when you configured the DNS proxy server using the **set system services dns dns-proxy view** *view-name* **domain** *domain-name* **forwarder** CLI statement, if the IP address specified in the forwarder option was not available, the DNS query was forwarded to the default DNS servers (DNS servers provided by the ISP). The device acquired the public IP addresses from the default DNS servers.

  Starting in Junos OS Release 12.1X46-D10, the **forward-only** option is added to the **set system services dns dns-proxy view** *view-name* **domain** *domain-name* **forward-only** CLI statement.

  You can use the **forward-only** option to prevent the device from acquiring the public IP addresses from the DNS servers (by terminating the DNS query) in cases when the specified IP address is unreachable.

Deprecated Items for High-End SRX Series Services Gateways

Table 7 on page 96 lists deprecated items (such as CLI statements, commands, options, and interfaces).

CLI statements and commands are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration. We strongly recommend that you phase out deprecated items and replace them with supported alternatives.

Table 7: Items Deprecated in Release 12.1

Deprecated Item	Replacement	Hierarchy Level or Command Syntax	Additional Information
download-timeout	-	download-timeout timeout	On all high-end SRX Series devices, the download-timeout command is deprecated. If the configuration is present, then the configuration is ignored. The IDP process internally triggers the security package to install when an automatic download is completed. There is no need to configure any download timeout.
node	-	request security idp security-package download	On all high-end SRX Series devices operating in a chassis cluster, the following request security idp security-package download commands with the node option are not supported: • request security idp security-package download node primary • request security idp security-package download node local • request security idp security-package download node all

Table 8: Items Deprecated in Junos OS Release 12.1X46

Deprecated Item	Replacement	Hierarchy Level or Command Syntax	Additional Information
mcc-mnc	imsi-prefix	edit security gprs gtp profile profile-name apn pattern-string	On all high-end SRX Series devices, the mcc-mnc command is not supported.

Table 9 on page 97 lists the deprecated system log messages in Junos OS Release 12.1X46.

Table 9: Deprecated System Log Messages in Junos OS Release 12.1X46

Deprecated Item	Replacement
RT_GTP_PKT_ECHO_REQUEST	RT_GTP_V0_PKT_ECHO_REQUEST
RT_GTP_PKT_ECHO_REPONSE	RT_GTP_V0_PKT_ECHO_RESPONSE
	RT_GTP_V1_PKT_ECHO_REQUEST
	RT_GTP_V1_PKT_ECHO_RESPONSE
	RT_GTP_V2_PKT_ECHO_REQUEST
	RT_GTP_V2_PKT_ECHO_RESPONSE

Compatibility

- **Version compatibility for Junos SDK**—Beginning with Junos OS Release 12.1X44-D10, Junos OS applications will install on the Junos OS only if the application is built with the same release as the Junos OS release on which the application is being installed.

  For example, an application built with Junos OS Release 12.1R2 will only install on Junos OS Release 12.1R2 and will not install on Junos OS Release 12.1R1 or Junos OS Release 12.1R3.

Flow and Processing

SPU software changes for the SPC—The following changes apply to all high-end SRX Series devices:

- Each SPU runs a 64-bit FreeBSD kernel instead of the 32-bit FreeBSD kernel.

- Each SPU runs a 64-bit flowd instead of the 32-bit version for increased scalability.

- With the 64-bit OS, ksynd and ifstates on the SPU run in 64-bit mode.

- **TCP initial timeout enhancement**—The minimum value you can configure for TCP session initialization is 4 seconds. The default value is 20 seconds; if required you can set the TCP session initialization value to less than 20 seconds.

- Starting with Junos OS Release 12.1X46-D10, you can configure the timeout value for a multicast flow session. In Junos OS Release 12.1X45-D10 and earlier, the timeout value for a multicast flow session was based on the packet IP protocol, which was not configurable.

  Multicast flow sessions have one template flow session and one or more leaf sessions. Because these sessions are linked together, they can have only one timeout value. The earlier implementation ignored the configurable timeout values of individual policies of each leaf session, and considered only the packet IP protocol timeout, which was not configurable. For example, for UDP this timeout value was always 60 seconds. As a result, multicast streams with a packet interval of more than 60 seconds experienced premature aging-out of flow sessions and packet drops.

  In the new implementation, multicast flow sessions consider the timeout values configured in leaf session policies along with the IP protocol timeout values. The highest

of these timeout values is selected as the template session timeout. You can configure the timeout value for the leaf session policy using custom applications.

[See *Configuring the Timeout Value for Multicast Flow Sessions*.]

• On all high end SRX Series devices, you can configure the TCP session timeout in a half-closed state by using the **apply-to-half-close-state** statement at the **[edit security flow tcp-session time-wait-state]** hierarchy level. This enables the system to apply the configured session timeout on receiving only one FIN packet (either client-to-server or server-to-client). When this statement is not configured, the default behavior takes effect, which is to apply the configured session timeout on receiving both the FIN packets. The default TCP session timeout remains 150 seconds. [See *apply-to-half-close-state*.]

J-Web

• On all high-end SRX Series devices, on the Monitoring Policies page, the Deactivate and Move functions on the toolbar and the Count and Log action columns in the output table are not supported and will no longer be available.

• On all high-end SRX Series devices, on the Checking Policies page, the Delete and Deactivate buttons are not supported and will no longer be available.

Logical Systems

- In Junos OS releases earlier than Junos OS Release 12.1X46-D10, when a logical tunnel interface with an IPv4 address and an Ethernet encapsulation type is configured, a configuration check is performed to ensure that the address is not identical to its peer logical tunnel interface address and that both addresses are on the same subnet. However, when a logical tunnel interface with an IPv6 address and an Ethernet encapsulation type is configured, no such configuration check is performed.

  Starting in Junos OS Release 12.1X46-D10, a check is performed for IPv6 configurations. However, this change can cause existing IPv6 configurations to fail.

Management Information Bases (MIBs)

- On all high-end SRX Series devices in a chassis cluster, the calculation of the primary and secondary node sessions in the JnxJsSPUMonitoringObjectsTable object of the SPU monitoring MIB is incorrect. The MIB JnxJsSPUMonitoringCurrentTotalSession incorrectly displays total sessions.

  A doubled session count is displayed because the active and backup nodes are treated as separate sessions, although these nodes are not separate sessions.

  Count only the session numbers on the local node, thereby avoiding a double count, and local total sessions are displayed.

  The SPUMonitoringCurrentTotalSession object of the MIB adds information per each SPU from the local node.

  [See *SNMP MIBS and Traps Reference for SRX1400 and SRX3000 Line Services Gateways*.]

  [See *SNMP MIBS and Traps Reference for SRX5000 Line Services Gateways*.]

Session Timeout for Reroute Failure

- The **route-change-timeout** configuration statement at the [**edit security flow**] hierarchy level sets the timeout when a session is rerouted but there is a reroute failure (for example, the new route uses a different egress zone from the previous route). In previous releases, the **route-change-timeout** statement was disabled by default. In Release 12.1X46-D10, the **route-change-timeout** configuration is enabled by default and the default timeout value is 6 seconds.

Simple Network Management Protocol (SNMP)

- On all high-end SRX Series devices, the screen SNMP trap **jnxJsScreenCfgChange** will not be sent during reboot.

System Logs

- In Junos OS Release 12.1X46-D10 and earlier, the session-id-32 in application volume tracing (AVT) logs were not prefixed with the spu-id, whereas the flow logs were prefixed with the spu-id.

Starting in Junos OS Release 12.1X46-D10 and later, that functionality has changed. The AVT logs are now prefixed with the spu-id, so that the session-ids in AVT logs are consistent with the flow logs and unique across the system.

The following example shows session-id-32 logging before Junos OS Release 12.1X46:

```
Oct  4 09:13:14  bournville RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed idle
 Timeout: 4.0.0.1/9->5.0.0.1/33631 icmp 4.0.0.1/9->5.0.0.1/33631 None None 1 1
 untrust trust 180000308 1(84) 0(0) 59 ICMP-ECHO UNKNOWN N/A(N/A) ge-0/0/0.0
UNKNOWN

Oct  4 09:13:14  bournville RT_FLOW: APPTRACK_SESSION_CLOSE: AppTrack session
closed idle Timeout: 4.0.0.1/9->5.0.0.1/33631 icmp ICMP-ECHO UNKNOWN
4.0.0.1/9->5.0.0.1/33631 None None 1 1 untrust trust 308 1(84) 0(0) 59 N/A N/A
 No
```

The following example shows session-id-32 logging in Junos OS Release 12.1X46-D10, indicating the fix in the flow and AVT logs:

```
Oct  4 13:57:38  bournville RT_FLOW: RT_FLOW_SESSION_CREATE: session created
4.0.0.1/58565->5.0.0.1/21 junos-ftp 4.0.0.1/58565->5.0.0.1/21 None None 6 1
untrust trust 180000001 N/A(N/A) ge-0/0/0.0 UNKNOWN UNKNOWN UNKNOWN

Oct  4 13:57:38  bournville RT_FLOW: APPTRACK_SESSION_CREATE: AppTrack session
 created 4.0.0.1/58565->5.0.0.1/21 junos-ftp UNKNOWN UNKNOWN
4.0.0.1/58565->5.0.0.1/21 None None 6 1 untrust trust 180000001 N/A N/A UNKNOWN
```

- On all high-end SRX Series devices, the attribute type of **packets-from-client** and **packets-from-server** options in the system logs of the following modules have been changed from unit to string:

  - App Track module— APPTRACK_SESSION_CLOSE, APPTRACK_SESSION_CLOSE_LS, APPTRACK_SESSION_VOL_UPDATE and APPTRACK_SESSION_VOL_UPDATE_LS

  - Session module—RT_FLOW_SESSION_CLOSE and RT_FLOW_SESSION_CLOSE_LS

On all high-end SRX Series devices, the following system log messages have been updated to include the **certificate ID**:

- PKID_PV_KEYPAIR_DEL

  Existing message: **Key-Pair deletion failed**

  New message: **Key-Pair deletion failed for <cert-id>**

- PKID_PV_CERT_DEL

  Existing message: **Certificate deletion has occurred**

  New message: **Certificate deletion has occurred for <cert-id>**

- PKID_PV_CERT_LOAD

  Existing message: **Certificate has been successfully loaded**

  New message: **Certificate <cert-id> has been successfully loaded**

- PKID_PV_KEYPAIR_GEN

  Existing message: **Key-Pair has been generated**

New message: **Key-Pair has been generated for <cert-id>**

Unified In-Service Software Upgrade (ISSU)

On all high-end SRX Series devices, at the beginning of a chassis cluster unified ISSU, the system automatically fails over all RG-1+ redundancy groups that are not primary on the node from which you start the ISSU. This action ensures that the redundancy groups are all active on only the RG-0 primary node. You no longer need to fail over redundancy groups manually.

After the system fails over all RG-1+ redundancy groups, the system sets the manual failover bit and changes all RG-1+ primary node priorities to 255, regardless of whether the redundancy group failed over to the RG-0 primary node.

Virtual Private Networks (VPNs)

- For each VPN tunnel, both ESP and AH tunnel sessions are installed on SPUs and the control plane. In previous Junos OS releases, two tunnel sessions of the same protocol (ESP or AH) were installed for each VPN tunnel. For branch SRX Series devices, tunnel sessions are updated with the negotiated protocol after negotiation is completed. For high-end SRX Series devices, tunnel sessions on anchor SPUs are updated with the negotiated protocol while non-anchor SPUs retain ESP and AH tunnel sessions.

  The ESP and AH tunnel sessions are displayed in the outputs for the **show security flow session** and **show security flow cp-session** operational mode commands.

- As of Junos OS Release 11.4, checks are performed to validate the IKE ID received from the VPN peer device. By default, SRX Series and J Series devices validate the IKE ID received from the peer with the IP address configured for the IKE gateway. In certain network setups, the IKE ID received from the peer (which can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address) does not match the IKE gateway configured on the SRX Series or J Series device. This can lead to a Phase 1 validation failure.

  To modify the configuration of the SRX Series or J Series device or the peer device for the IKE ID that is used:

  - On the SRX Series or J Series device, configure the **remote-identity** statement at the [**edit security ike gateway** *gateway-name*] hierarchy level to match the IKE ID that is received from the peer. Values can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address.

    NOTE: If you do not configure remote-identity, the device uses the IPv4 or IPv6 address that corresponds to the remote peer by default.

  - On the peer device, ensure that the IKE ID is the same as the **remote-identity** configured on the SRX Series or J Series device. If the peer device is an SRX Series or J Series device, configure the **local-identity** statement at the [**edit security ike gateway** *gateway-name*] hierarchy level. Values can be an IPv4 or IPv6 address, fully qualified domain name, distinguished name, or e-mail address.

- On all high-end SRX Series devices, the subject fields of a digital certificate can include Domain Component (DC), Common Name (CN), Organization Unit (OU), Organization (O), Location (L), State (ST), and Country (C).

  In earlier releases, the **show security pki ca-certificate** and **show security pki local-certificate** CLI operational commands displayed only a single entry for each subject field, even if the certificate contained multiple entries for a field.

  For example, a certificate with two OU fields such as "OU=Shipping Department, OU=Priority Mail" displayed only the first entry "OU=Shipping Department." The **show security pki ca-certificate** and **show security pki local-certificate** CLI commands now display the entire contents of the subject field, including multiple field entries. The commands also display a new subject string output field that shows the contents of the subject field as it appears in the certificate.

- PKI objects include certificates, key pairs, and CRLs. PKI objects are read from the PKI database when the PKI Daemon starts. The PKI Daemon database loads all certificates into memory at boot time.

  When an object is read into memory from the PKI database, the following new log message is created:

  PKID_PV_OBJECT_READ: A PKI object was read into memory from <location>

Related Documentation

- New and Changed Features on page 78
- Known Issues on page 121
- Resolved Issues on page 126
- Documentation Updates on page 134
- Known Behavior on page 102

Known Behavior

Application Layer Gateways (ALGs)

- The maximum size of the jbuf is 9 Kb. If the message buffer size is more than 9 Kb, the entire message cannot be transferred to the ALG packet handler. This causes subsequent packets in the session to bypass ALG handling, resulting in a transaction failure.

The limitations for SCCP ALGs are as follows:

- The SCCP is a Cisco proprietary protocol. So, any changes to the protocol by Cisco cause the SCCP ALG implementation to break. However, workarounds are provided to bypass strict decoding and allow any protocol changes to be handled gracefully.

- The SCCP ALG validates protocol data units (PDUs) with message IDs in the ranges [0x0 - 0x12], [0x20 - 0x49], and [0x81 - 0x14A]. By default, all other message IDs are treated as unknown messages and are dropped by the SCCP ALG.

- Any changes to the policies will drop the sessions and impact already established SCCP calls.

- The SCCP ALG opens pinholes that are collapsed during traffic or media inactivity. This means that during a temporary loss of connectivity, media sessions are not re-established.

- CallManager (CM) version 6.x and later does not support TCP probe packets in chassis cluster mode. As a result, the existing SCCP sessions will break when there is a failover. You can still create new SCCP sessions during failover.

The PPTP ALG with IPv6 support has the following limitation:

- Because PPP packets are compressed with Microsoft Point-to-Point Encryption (MPPE) protocol after the tunnel is set up, translation of the IP header in the PPP package cannot be handled; therefore, to make sure PPTP connection works well, the PPTP client must be able to work in dual stack mode. So that an IPv6 PPTP client can accept an IPv4 address for PPP tunnel interface, by which it can communicate with the IPv4 PPTP server without IP address translation for PPP packets.

The RTSP ALG with IPv6 support has the following limitations:

- Real-Time Streaming Protocol (RTSP) is an Application Layer protocol for controlling the delivery of data with real-time properties. The RTSP ALG supports a peer client, and the server transmits real-time media; it does not support third-party endpoints involved in the transaction.

- In case of destination NAT or NAT64 for IP address translation, if the RTSP message (including the Session Description Protocol (SDP) application content) length exceeds 2500 bytes, then the RTSP ALG processes only the first 2500 bytes of the message and ignores the rest of the message. In this scenario, the IP address in the RTSP message is not translated if the IP address does not appear in the first 2500 bytes.

The SIP ALG with IPv6 support has the following limitation:

- When NAT64 with persistent NAT is implemented, the SIP ALG adds the NAT translation to the persistent NAT binding table if NAT is configured on the Address of Record (AOR). Because persistent NAT cannot duplicate the address configured, coexistence of NAT66 and NAT64 configured on the same address is not supported.

  Only one binding is created for the same source IP address.

AppSecure

- J-Web pages for AppSecure are preliminary.

- Custom application signatures and custom nested application signatures are not currently supported by J-Web.

- When ALG is enabled, application identification includes the ALG result to identify the application of the control sessions. Application firewall permits ALG data sessions whenever control sessions are permitted. If the control session is denied, there are no data sessions.

  When ALG is disabled, application identification relies on its signatures to identify the application of the control and data sessions. If a signature match is not found, the

application is considered unknown. Application firewall handles applications based on the application identification result.

Chassis Cluster

- If you are adding next-generation SRX5K-SPC-4-15-320 SPCs on SRX5600 and SRX5800 devices that are part of a chassis cluster, you must install the new SPCs so that a next-generation SRX5K-SPC-4-15-320 SPC is the SPC in the original lowest-numbered slot. For example, if the chassis already has two first-generation SRX5K-SPC-2-10-40 SPCs installed in slots 2 and 3, you cannot install SRX5K-SPC-4-15-320 SPCs in slot 0 or 1. You will need to make sure that an SRX5K-SPC-4-15-320 SPC is installed in the slot that provides central point functionality (in this case, slot 2). This ensures that the central point functionality is performed by an SRX5K-SPC-4-15-320 SPC.

- On all high-end SRX Series devices, IPsec VPN is not supported in active/active chassis cluster configuration (that is, when there are multiple RG1+ redundancy groups).

The following list describes the limitations for inserting an SPC on SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices in chassis cluster mode:

- The chassis cluster must be in active/passive mode before and during the SPC insert procedure.

- A different number of SPCs cannot be inserted in two different nodes.

- A new SPC must be inserted in a slot that is higher than the central point slot.

> NOTE: The existing combo central point cannot be changed to a full central point after the new SPC is inserted.

- During an SPC insert procedure, the IKE and IPsec configurations cannot be modified.

- Users cannot specify the SPU and the IKE instance to anchor a tunnel.

- After a new SPC is inserted, the existing tunnels cannot use the processing power of the new SPC and redistribute it to the new SPC.

- Dynamic tunnels cannot load-balance across different SPCs.

- The manual VPN name and the site-to-site gateway name cannot be the same.

- In a chassis cluster scaling environment, the heartbeat-threshold must always be set to 8.

- An APN or an IMSI filter must be limited to 600 for each GTP profile. The number of filters is directly proportional to the number of IMSI prefix entries. For example, if one APN is configured with two IMSI prefix entries, then the number of filters is two.

- Eight QoS queues are supported per ae interface.

- The first recommended unified ISSU *from* release is Junos OS Release 10.4R4. If you intend to upgrade from a release earlier than Junos OS Release 10.4R4, see the release

notes for the release that you are upgrading *from* for information about limitations and issues related to upgrading.

- Unified ISSU does not support the following features:

  - DHCP

  - GPRS, GTP, and SCTP

  - Flow monitoring

  For the latest unified ISSU support status, go to the Juniper Networks Knowledge Base (KB): http://kb.juniper.net/ and search for KB17946.

- Unified ISSU does not support version downgrading.

- In large chassis cluster configurations on SRX1400, SRX3400 or SRX3600 devices, you need to increase the wait time before triggering failover. In a full-capacity implementation, we recommend increasing the wait to 8 seconds by modifying **heartbeat-threshold** and **heartbeat-interval** values in the **[edit chassis cluster]** hierarchy.

  The product of the **heartbeat-threshold** and **heartbeat-interval** values defines the time before failover. The default values (**heartbeat-threshold** of 3 beats and **heartbeat-interval** of 1000 milliseconds) produce a wait time of 3 seconds.

  To change the wait time, modify the option values so that the product equals the desired setting. For example, setting the **heartbeat-threshold** to 8 and maintaining the default value for the **heartbeat-interval** (1000 milliseconds) yields a wait time of 8 seconds. Likewise, setting the **heartbeat-threshold** to 4 and the **heartbeat-interval** to 2000 milliseconds also yields a wait time of 8 seconds.

- Packet-based forwarding for MPLS and ISO protocol families is not supported.

- On SRX5600 and SRX5800 devices, only two of the 10 ports on each PIC of 40-port 1-Gigabit Ethernet I/O cards (IOCs) can simultaneously enable IP address monitoring. Because there are four PICs per IOC, this permits a total of eight ports per IOC to be monitored. If more than two ports per PIC on 40-port 1-Gigabit Ethernet IOCs are configured for IP address monitoring, the commit will succeed but a log entry will be generated, and the accuracy and stability of IP address monitoring cannot be ensured. This limitation does not apply to any other IOCs or devices.

- IP address monitoring is not supported on reth interface link aggregation groups (LAGs) or on child interfaces of reth interface LAGs.

- Screen statistics data can be gathered on the primary device only.

- Only reth interfaces are supported for IKE external interface configuration in IPsec VPN. Other interface types can be configured, but IPsec VPN might not work.

Dynamic Host Configuration Protocol (DHCP)

- On all high-end SRX Series devices, DHCPv6 client authentication is not supported.

- On all high-end SRX Series devices, DHCP is not supported in a chassis cluster.

- On all high-end SRX Series devices, DHCP relay is unable to update the binding status based on DHCP_RENEW and DHCP_RELEASE messages.

Flow and Processing

- On all high-end SRX Series devices, when packet-logging functionality is configured with an improved pre-attack configuration parameter value, the resource usage increases proportionally and might affect the performance.

- On all high-end SRX Series devices, the default authentication table capacity is 45,000; the administrator can increase the capacity to a maximum of 50,000.

  On SRX1400 devices, the default authentication table capacity is 10,000; the administrator can increase the capacity to a maximum of 15,000.

- On all high-end SRX Series devices, when devices are operating in flow mode, the Routing Engine side cannot detect the path MTU of an IPv6 multicast address (with a large size packet).

- On all high-end SRX Series devices, you cannot configure route policies and route patterns in the same dial plan.

- On all high-end SRX Series devices, high CPU utilization triggered for reasons such as CPU intensive commands and SNMP walks causes the BFD protocol to flap while processing large BGP updates.

- On all high-end SRX Series devices, downgrading is not supported in low-impact unified ISSU chassis cluster upgrades (LICU).

- On SRX5800 devices, network processing bundling is not supported in Layer 2 transparent mode.

General Packet Radio Service (GPRS)

The following Gateway GPRS Support Node (GGSN) and Packet Data Network Gateway (PGW) limitations are applicable for all high-end SRX Series devices.

- GGSN and PGW traffic must pass through the GPRS tunneling protocol (GTP) framework; otherwise, the tunnel status is updated incorrectly.

- The central point distributes all GTP packets to SPUs according to upstream endpoints for GGSN or PGW (one GGSN or PGW is the upstream endpoint of the GTP tunnels). Information is checked on the upstream endpoint IP and GTP packets in the GGSN pool network in the following way:

- If the upstream endpoint source IP address in the Create-PDP-Context-Response or Create-Session-Response message is different from the IP address of the upstream endpoint, tunnels are created on one SPU. According to the IP address of the upstream endpoint for GGSN or PGW, an incoming GTP tunnel message is moved to a second SPU, and the GTP packets are dropped because no tunnel is found.

  NOTE: In the GGSN pool scenario, GGSN can reply with a Create-PDP-Context-Request or Create-Session-Request message using another IP address that differs from the one received. Therefore the request and the response can run on two different flow sessions, and these two flow sessions can be distributed to different SPUs.

The following GTP firewall limitations are applicable on all high-end SRX Series devices.

- GTP firewall does not support hot-insertable and hot-removable hardware.

- Unified ISSU is not supported from an earlier release to the current release.

- The GTP firewall needs to learn the network's GSN table and install the table for the central point and the SPU. Otherwise, some GTP traffic is blocked when the firewall is inserted in the network.

- On all high-end SRX Series devices, the GPRS tunneling protocol (GTP) module competes with other modules for memory allocation during runtime because it has dynamic memory allocation for tunnel management.

- On all high-end SRX Series devices, GTP-U inspection has the following limitations:

  - When GTP-U inspection is enabled, GTP-U throughput drops.

  - GTP-U inspection only affects the new flow sessions that are created after enabling the GTP-U inspection.

    NOTE: When GTP-U inspection is disabled, the GTP module ignores the traffic on which the corresponding flow sessions were created. When GTP-U inspection is reenabled, the GTP module continues to ignore the traffic during the lifetime of the flow sessions that were created before the GTP-U inspection was reenabled.

  - The ramp-up rate of GTP tunnel management messages decreases slightly (the decrease rate is less than 10 percent) when the GTP control (GTP-C) tunnel and GTP-U tunnel are created on different SPUs, whether GTP-U inspection is enabled or not.

- On all high-end SRX Series devices, NAT for GTP packets has the following limitations:

  - Only static NAT is supported; port NAT is not supported.

  - During a packet data protocol (PDP) context negotiation and update, the packet sent from the customer's GSNs must carry the public IP in the GTP payload.

- Source IP and destination IP addresses cannot be translated simultaneously for a packet.

- NAT for GTP only works in default logical systems.

- IPv6 is not supported.

The following SCTP limitations are applicable on all high-end SRX Series devices:

- Dynamic policy is not supported for SCTP. You must configure all policies for needed SCTP sessions.

- SCTP modules only inspect IPv4 traffic. IPv6 traffic will be passed or dropped by flow-based or policy-based processing directly, and no SCTP module inspection will occur.

- Only the first chunk in each SCTP packet is checked.

- For static NAT to work, the interfaces packets (from one side: client or server side) coming in must belong to the same zone.

- For multihome cases, only IPv4 Address Parameter (5) in INIT or INI-ACK is supported.

- Only static NAT is supported for SCTP.

- SCTP enable or disable is controlled by whether there is a SCTP profile configured. When you disable the SCTP feature, all associations are deleted and later SCTP packets will pass or drop according to the policy.

  If you want to enable SCTP again, all the running SCTP communications will be dropped, because no associations exist. New SCTP communications can establish an association and perform the inspections.

  Clear old SCTP sessions when SCTP is reenabled; doing this will avoid any impact caused by the old SCTP sessions on the new SCTP communications.

- Only established SCTP associations will be synchronized to peer node.

- A maximum of eight source IP addresses and eight destination IP addresses are allowed in an SCTP communication.

- One SPU supports a maximum of 5000 associations and a maximum of 320, 000 SCTP sessions.

- The 4-way handshake process should be done in one node of a cluster. If the SCTP 4-way handshake process is handled on two nodes (for example, two sessions on two nodes in active/active mode) or the cluster fails over before the 4-way handshake is finished, the association cannot be established successfully.

- If you configure different policies for each session belonging to one association, there will be multiple policies related to one association. The SCTP packet management (drop, rate limit, and so on) will use the profile attached to the handling SCTP session's policy.

  The association's timeout will only use the profile attached to its INIT packet's policy. If the INIT packet's policy changes the attached profile, the old profile is deleted, and the association will refresh the timeout configuration. However, if the INIT packet's

policy changes its attached profile without deleting the old profile, the association will not refresh the timeout configuration.

- Unified ISSU to earlier Junos OS releases is not supported.

- In some cases, the associations might not be distributed to SPUs very evenly because the port's hash result on the central point is uneven. For example, this event can occur when only two peers of ports are used, and one peer has 100 associations, but another peer has only one association. In this case, the associations cannot be distributed evenly on the firewall with more than one SPU.

- SCTP sessions will not be deleted with associations, and the sessions will time out in 30 minutes, which is the default value. If you need the session to time out soon, you can preconfigure the SCTP application timeout value.

- M3UA or SCCP message parsing is checked , but the M3UA or SCCP stateful inspection is not checked.

- Only ITU-T Rec. Q.711-Q.714 (07 or 96) standard is supported. ANSI, ETSI, China, and other standards are not supported.

- Only RFC 4960 is supported.

On all high-end SRX Series devices, SCTP payload protocol blocking has the following limitations:

- The supported protocol decimal value is from 0 to 63. This value includes 48 IANA assigned protocols and 16 unassigned protocols.

- When running SCTP data traffic during a unified ISSU, the SCTP data packets are dropped at Junos OS Release 12.1X46. Only after the unified ISSU is finished, you can configure **permit** on Junos OS Release 12.1X46-D10 and pass the SCTP data traffic.

- Only the first data chunk is inspected, so protocol blocking only works for the first data chunk.

On all high-end SRX Series devices, the SCTP rate limiting function has the following limitations:

- The supported protocol decimal value is from 0 to 63. This value includes 48 IANA assigned protocols and 16 unassigned protocols.

- Only the first data chunk is inspected, so the rate limiting function only works for the first data chunk.

- A maximum of 80 addresses are rate limited in one profile.

- A maximum of 10 protocols are rate limited for one address in one profile.

- The supported rate limit value is from 1 to 12000.

Hardware

- SRX5800 devices does not support a redundant SCB card (third SCB) if an SRX5k SPC II (FRU model number: SRX5K-SPC-4-15-320) is installed on the device. If you have installed an SRX5k SPC II on an SRX5800 device with a redundant SCB card, make sure to remove the redundant SCB card.

Interfaces and Routing

This section covers filter and policing limitations.

- On SRX1400, SRX3400, and SRX3600 devices, the following feature is not supported by a simple filter:

  - Forwarding class as match condition

- On SRX1400, SRX3400 and SRX3600, devices, the following features are not supported by a policer or a three-color-policer:

  - Color-aware mode of a three-color-policer

  - Filter-specific policer

  - Forwarding class as action of a policer

  - Logical interface policer

  - Logical interface three-color policer

  - Logical interface bandwidth policer

  - Packet loss priority as action of a policer

  - Packet loss priority as action of a three-color-policer

- On all high-end SRX Series devices, the following features are not supported by a firewall filter:

  - Policer action

  - Egress filter-based forwarding (FBF)

  - Forwarding table filter (FTF)

- SRX3400 and SRX3600 devices have the following limitations of a simple filter:

  - The forwarding class is the match condition.

  - In the packet processor on an IOC, up to 400 logical interfaces can be applied with simple filters.

  - In the packet processor on an IOC, the maximum number of terms of all simple filters is 2000.

  - In the packet processor on an IOC, the maximum number of policers is 2000.

- In the packet processor on an IOC, the maximum number of three-color-policers is 2000.

- The maximum burst size of a policer or three-color-policer is 16 MB.

- On all high-end SRX Series devices, the flow monitoring version 9 has the following limitations:

  - Routing Engine based flow monitoring V5 or V8 mode is mutually exclusive with inline flow monitoring V9.

  - High-end SRX Series devices do not support multiple collectors like branch SRX Series devices. Only one V9 collector per IPv4 or IPv6 is supported.

  - Flow aggregation for V9 export is not supported.

  - Only UDP over IPv4 or IPv6 protocol can be used as the transport protocol.

  - Only the standard IPv4 or IPv6 template is supported for exporting flow monitoring records.

  - User-defined or special templates are not supported for exporting flow monitoring records.

  - Chassis cluster is supported without flow monitoring session synchronization.

- On SRX3400 and SRX3600 devices, when you enable the monitor traffic option using the **monitor traffic** command to monitor the FXP interface traffic, interface bounce occurs. You must use the **monitor traffic interface fxp0 no-promiscuous** command to avoid the issue.

- On all high-end SRX Series devices, the lo0 logical interface cannot be configured with RG0 if used as an IKE gateway external interface.

- On all high-end SRX Series devices, the **set protocols bgp family inet flow** and **set routing-options flow** CLI statements are no longer available, because BGP flow spec functionality is not supported on these devices.

- On all high-end SRX Series devices, the LACP is not supported on Layer 2 interfaces.

- On all high-end SRX Series devices, BGP-based virtual private LAN service (VPLS) works on child ports and physical interfaces, but not over ae interfaces.

Intrusion Detection and Prevention (IDP)

- On all high-end SRX Series devices, from Junos OS Release 11.2 and later, the IDP security package is based on the Berkeley database. Hence, when the Junos OS image is upgraded from Junos OS Release 11.1 or earlier to Junos OS Release 11.2 or later, a migration of IDP security package files needs to be performed. This is done automatically on upgrade when the IDP process comes up. Similarly, when the image is downgraded, a migration (secDb install) is automatically performed when the IDP process comes up, and previously installed database files are deleted.

  However, migration is dependent on the XML files for the installed database present on the device. For first-time installation, completely updated XML files are required. If the last update on the device was an incremental update, migration might fail. In such

a case, you have to manually download and install the IDP security package using the **download** or **install** CLI commands before using the IDP configuration with predefined attacks or groups.

As a workaround, use the following CLI commands to manually download the individual components of the security package from the Juniper Security Engineering portal and install the full update:

- **request security idp security-package download full-update**

- **request security idp security-package install**

- On all high-end SRX Series devices, the IDP policies for each user logical system are compiled together and stored on the data plane memory. To estimate adequate data plane memory for a configuration, consider these two factors:

  - IDP policies applied to each user logical system are considered unique instances because the ID and zones for each user logical system are different. Estimates need to consider the combined memory requirements for all user logical systems.

  - As the application database increases, compiled policies requires more memory. Memory usage should be kept below the available data plane memory to allow for database increases.

- On all high-end SRX Series devices, ingress as ge-0/0/2 and egress as ge-0/0/2.100 works with flow showing both source and destination interface as ge-0/0/2.100.

- IDP does not allow header checks for nonpacket contexts.

- On all high-end SRX Series devices, application-level distributed denial-of-service (application-level DDoS) detection does not work if two rules with different application-level DDoS applications process traffic going to a single destination application server. When setting up application-level DDoS rules, make sure that you do not configure rulebase-ddos rules that have two different application-ddos objects when the traffic destined to one application server can process more than one rule. Essentially, for each protected application server, you have to configure the application-level DDoS rules so that traffic destined for one protected server processes only one application-level DDoS rule.

    NOTE: Application-level DDoS rules are terminal, which means that once traffic is processed by one rule, it will not be processed by other rules.

    The following configuration options can be committed, but they will not work properly:

source-zone	destination-zone	destination-ip	service	application-ddos	Application Server
source-zone-1	dst-1	any	http	http-appddos1	1.1.1.1:80
source-zone-2	dst-1	any	http	http-appddos2	1.1.1.1:80

- On all high-end SRX Series devices, application-level DDoS rule base (rulebase-ddos) does not support port mapping. If you configure an application other than default, and if the application is from either predefined Junos OS applications or a custom application that maps an application service to a nonstandard port, application-level DDoS detection will not work.

  When you configure the application setting as default, IDP uses application identification to detect applications running on standard and nonstandard ports; thus, the application-level DDoS detection would work properly.

- On all high-end SRX Series devices, all IDP policy templates are supported except All Attacks. There is a 100-MB policy size limit for integrated mode and a 150-MB policy size limit for dedicated mode. The current IDP policy templates supported are dynamic, based on the attack signatures being added. Therefore, be aware that supported templates might eventually grow past the policy size limit.

  On all high-end SRX Series devices, the following IDP policies are supported:

  - DMZ_Services

  - DNS_Service

  - File_Server

  - Getting_Started

  - IDP_Default

  - Recommended

  - Web_Server

- IDP deployed in both active/active and active/passive chassis clusters has the following limitations:

  - No inspection of sessions that fail over or fail back.

  - The IP action table is not synchronized across nodes.

  - The Routing Engine on the secondary node might not be able to reach networks that are reachable only through a Packet Forwarding Engine.

  - The SSL session ID cache is not synchronized across nodes. If an SSL session reuses a session ID and it happens to be processed on a node other than the one on which the session ID is cached, the SSL session cannot be decrypted and will be bypassed for IDP inspection.

- IDP deployed in active/active chassis clusters has a limitation that for time-binding scope source traffic, if attacks from a source (with more than one destination) have active sessions distributed across nodes, then the attack might not be detected because time-binding counting has a local-node-only view. Detecting this sort of attack requires an RTO synchronization of the time-binding state that is not currently supported.

IPv6

IPv6 IPsec implementation has the following limitations:

- Devices with IPv6 addressing do not perform fragmentation. IPv6 hosts should either perform path MTU discovery or send packets smaller than the IPv6 minimum MTU size of 1280 bytes.

- Because IPv6 addresses are 128 bits long compared to IPv4 addresses, which are 32-bits long, IPv6 IPsec packet processing requires more resources. Therefore, a small performance degradation is observed.

- IPv6 uses more memory to set up the IPsec tunnel. Therefore, the IPsec IPv4 tunnel scalability numbers might drop.

- The addition of IPv6 capability might cause a drop in the IPsec IPv4-in-IPv4 tunnel throughput performance.

- The IPv6 IPsec VPN does not support the following functions:

    - 4in6 and 6in4 policy-based site-to-site VPN, IKE

    - 4in6 and 6in4 route-based site-to-site VPN, IKE

    - 4in6 and 6in4 policy-based site-to-site VPN, Manual Key

    - 4in6 and 6in4 route-based site-to-site VPN, Manual Key

    - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, IKE

    - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, Manual Key

    - Remote Access—XAuth, config mode, and shared IKE identity with mandatory XAuth

    - IKE authentication—PKI or DSA

    - IKE peer type—dynamic IP

    - Chassis cluster for basic VPN features

    - IKE authentication—PKI or RSA

    - NAT-T

    - VPN monitoring

    - Hub-and-spoke VPNs

    - NHTB

    - DPD

    - SNMP for IPsec VPN MIBs

    - Chassis cluster for advanced VPN features

    - IPv6 link-local address

- **Network and Security Manager (NSM)**—Consult the NSM release notes for version compatibility, required schema updates, platform limitations, and other specific details regarding NSM support for IPv6 addressing on all high-end SRX Series devices.

- **Security policy**—Only IDP for IPv6 sessions is supported for all high-end SRX Series devices. UTM for IPv6 sessions is not supported. If your current security policy uses rules with the IP address wildcard any, and UTM features are enabled, you will encounter configuration commit errors because UTM features do not yet support IPv6 addresses. To resolve the errors, modify the rule returning the error so that the any-ipv4 wildcard is used; and create separate rules for IPv6 traffic that do not include UTM features.

J-Web

- The following table indicates browser compatibility:

Table 10: Browser Compatibility on High-End SRX Series Devices

Device	Application	Supported Browsers	Recommended Browser
SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800	J-Web	• Mozilla Firefox version 3.6 or later • Microsoft Internet Explorer version 7.0	Mozilla Firefox version 3.6 or later

- To use the Chassis View, a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9) must be installed. Also note that the Chassis View is displayed by default on the Dashboard page. You can enable or disable the Chassis View using options in the dashboard Preference dialog box, but clearing cookies in Microsoft Internet Explorer also causes the Chassis View to be displayed.

- On all high-end SRX Series devices, users cannot differentiate between Active and Inactive configurations on the System Identity, Management Access, User Management, and Date & Time pages.

Logical Systems

- The master logical system must not be bound to a security profile that is configured with a 0 percent reserved CPU quota because traffic loss could occur. When upgrading all high-end SRX Series devices from Junos OS Release 11.2, make sure that the reserved CPU quota in the security profile that is bound to the master logical system is configured for 1 percent or more. After upgrading from Junos OS Release 11.2, the reserved CPU quota is added to the default security profile with a value of 1 percent.

- On all high-end SRX Series devices, quality-of-service (QoS) classification across interconnected logical systems does not work.

- On all high-end SRX Series devices, the number of logical system security profiles you can create is constrained by an internal limit on security profile IDs. The security profile ID range is from 1 through 32, with ID 0 reserved for the internally configured default security profile. When the maximum number of security profiles is reached, if you want to add a new security profile, you must first delete one or more existing security profiles, commit the configuration, and then create the new security profile and commit it. You cannot add a new security profile and remove an existing one within a single configuration commit.

If you want to add more than one new security profile, the same rule is true. You must first delete the equivalent number of existing security profiles, commit the configuration, and then create the new security profiles and commit them.

- **User and administrator configuration for logical systems**—Configuration for users for all logical systems and all user logical systems administrators must be done at the root level by the master administrator. A user logical system administrator cannot create other user logical system administrators or user accounts for their logical systems.

- **Name-space separation**—The same name cannot be used in two logical systems. For example, if logical-system1 includes the username "Bob" then other logical systems on the device cannot include the username "Bob".

- **Commit rollback**—Commit rollback is supported at the root level only.

- **Trace and debug**—Trace and debug are supported at the root level only.

- **Class of service**—You cannot configure class of service on logical tunnel (lt-0/0/0) interfaces.

- **ALGs**—The master administrator can configure ALGs at the root level. The configuration is inherited by all user logical systems. It cannot be configured discretely for user logical systems.

Network Address Translation (NAT)

- **Single IP address in a source NAT pool without PAT**—The number of hosts that a source NAT pool without PAT can support is limited to the number of addresses in the pool. When you have a pool with a single IP address, only one host can be supported, and traffic from other hosts is blocked because there are no resources available.

  If a single IP address is configured for a source NAT pool without PAT when NAT resource assignment is not in active-backup mode in a chassis cluster, traffic through node 1 will be blocked.

- For all ALG traffic, except FTP, we recommend that you not use the static NAT rule options **source-address** or **source-port**. Data session creation can fail if these options are used, because the IP address and the source port value, which is a random value, might not match the static NAT rule. For the same reason, we also recommend that you not use the source NAT rule option **source-port** for ALG traffic.

  For FTP ALG traffic, the **source-address** option can be used because an IP address can be provided to match the source address of a static NAT rule.

  Additionally, because static NAT rules do not support overlapping addresses and ports, they should not be used to map one external IP address to multiple internal IP addresses for ALG traffic. For example, if different sites want to access two different FTP servers, the internal FTP servers should be mapped to two different external IP addresses.

- On all high-end SRX Series devices, in case of SSL proxy, sessions are whitelisted based on the actual IP address and not on the translated IP address. Because of this, in the whitelist configuration of the SSL proxy profile, the actual IP address should be provided and not the translated IP addresses.

Example:

Consider a destination NAT rule that translates destination IP address 20.20.20.20 to 5.0.0.1 using the following commands:

- **set security nat destination pool d1 address 5.0.0.1/32**

- **set security nat destination rule-set dst-nat rule r1 match destination-address 20.20.20.20/32**

- **set security nat destination rule-set dst-nat rule r1 then destination-nat pool d1**

In the above scenario, to exempt a session from SSL proxy inspection, the following IP address should be added to the whitelist:

- **set security address-book global address ssl-proxy-exempted-addr 20.20.20.20/32**

- **set services ssl proxy profile ssl-inspect-profile whitelist ssl-proxy-exempted-addr**

- Maximum capacities for source pools and IP addresses have been extended on all high-end SRX Series devices as follows:

Pool/PAT Maximum Address Capacity	SRX1400	SRX3400 SRX3600	SRX5400 SRX5600 SRX5800
Source NAT pools	8192	8192	12,288
IP addresses supporting port translation	8192	8192	12,288
PAT port number	256M	256M	384M

Increasing the capacity of source NAT pools consumes memory needed for port allocation. When source NAT pool and IP address limits are reached, port ranges should be reassigned. That is, the number of ports for each IP address should be decreased when the number of IP addresses and source NAT pools is increased. This ensures NAT does not consume too much memory. Use the **port-range** statement in configuration mode in the CLI to assign a new port range or the **pool-default-port-range** statement to override the specified default.

Configuring port overloading should also be done carefully when source NAT pools are increased.

For source pool with PAT in range (63,488 through 65,535), two ports are allocated at one time for RTP or RTCP applications, such as SIP, H.323, and RTSP. In these scenarios, each IP address supports PAT, occupying 2048 ports (63,488 through 65,535) for ALG module use. On SRX5600 and SRX5800 devices, if all of the 12288 source pool is configured, a port allocation of 2M is reserved for twin port use.

- **NAT rule capacity change**—To support the use of large-scale NAT at the edge of the carrier network, the device wide NAT rule capacity has been changed.

The number of destination, static, and source NAT rules has been incremented as shown in . The limitation on the number of destination rule sets and static rule sets has been increased.

provides the requirements per device to increase the configuration limitation as well as to scale the capacity for each device.

Table 11: Number of Rules on All High-End SRX Series Devices

NAT Rule Type	SRX1400	SRX3400 SRX3600	SRX5400 SRX5600 SRX5800
Source NAT rule	8192	20480	30720
Destination NAT rule	8192	20480	30720
Static NAT rule	8192	20480	30720

The restriction on the number of rules per rule set has been increased so that there is only a devicewide limitation on how many rules a device can support. This restriction is provided to help you better plan and configure the NAT rules for the device.

For memory consumption, there is no guarantee to support these numbers (maximum source rule or rule set + maximum destination rule or rule set + maximum static rule or rule-set) at the same time for SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.

The suggested total number of rules and rule sets is listed in following table:

Objects	SRX3400 SRX3600	SRX5400 SRX5600 SRX5800
Total NAT rule sets per system	20,480	30,720
Total NAT rules per rule set	20,480	30,720

Security Policies

- On all high-end SRX Series devices, the current SSL proxy implementation has the following connectivity limitations:

    - The SSLv2 protocol is not supported. SSL sessions using SSLv2 are dropped.

    - SSL sessions where client certificate authentication is mandatory are dropped.

    - SSL sessions where renegotiation is requested are dropped.

- On all high-end SRX Series devices, for a particular session, the SSL proxy is only enabled if a relevant feature related to SSL traffic is also enabled. Features that are related to SSL traffic are IDP, application identification, application firewall, and

application tracking. If none of the above listed features are active on a session, the SSL proxy bypasses the session and logs are not generated in this scenario.

- On all high-end SRX Series devices, you cannot configure the following IP addresses as negated addresses in a policy:

  - Wildcard addresses

  - IPv6 addresses

  - Addresses such as **any**, **any-ipv4** , **any-IPv6** and **0.0.0.0**

- When a range of addresses or a single address is negated, it can be divided into multiple addresses. These negated addresses are shown as a prefix or a length that requires more memory for storage on a Packet Forwarding Engine.

- Each platform has a limited number of policies with negated addresses. A policy can contain 10 source or destination addresses. The capacity of the policy depends on the maximum number of policies that the platform supports.

Services Offloading

- Services offloading has the following limitations:

  - Transparent mode is not supported. If transparent mode is configured, a normal session is installed.

  - LAG is not supported. If a LAG is configured, a normal session is installed.

  - Only multicast sessions with one fan-out are supported. If a multicast session with more than one fan-out exists, a normal session is installed.

  - Only active/passive chassis cluster configuration is supported. Active/active chassis cluster configuration is not supported.

  - Fragmented packets are not supported. If fragmented packets exist, a normal session is installed.

  - IPv6 is not supported. If IPv6 is configured, a normal session is installed.

  > NOTE: A normal session forwards packets from the network processor to the SPU for fast-path processing. A services-offload session processes fast-path packets in the network processor and the packets exit out of the network processor itself.

- For Non-Services-Offload Sessions:

  - When services offloading is enabled, for normal sessions, the performance can drop by approximately 20 percent for connections per second (CPS) and 15 percent for packets per second (pps) when compared with non-services-offload mode.

  - For Services-Offload Sessions:

    When services offloading is enabled, for fast-forward sessions, the performance can drop by approximately 13 percent for connections per second (CPS).

Simple Network Management Protocol (SNMP)

- On all high-end SRX Series devices, the **show snmp mib** CLI command will not display the output for security related MIBs. We recommend that you use an SNMP client and prefix **logical-system-name@** to the community name. For example, if the community is **public**, use **default@public** for default root logical system.

Virtual Private Networks (VPNs)

On all high-end SRX Series devices, IKEv2 does not include support for:

- Policy-based tunnels

- Dial-up tunnels

- Network Address Translation-Traversal (NAT-T)

- VPN monitoring

- NHTP for st0—Reusing the same tunnel interface for multiple tunnels

- EAP

- Multiple child SAs for the same traffic selectors for each QoS value

- Proposal enhancement features

- Reuse of Diffie-Hellman (DH) exponentials

- Configuration payloads

- IP Payload Compression Protocol (IPComp)

- Dynamic endpoint (DEP) VPN

- VPN monitoring and Suite B cryptographic configuration options **ecdsa-signatures-384** (for IKE authentication) and Diffie-Hellman **group20** consume considerable CPU resources. If VPN monitoring and the **ecdsa-signatures-384** and **group20** options are used on an SRX Series device with a large number of tunnels configured, the device must have the next-generation SPC installed.

- On all high-end SRX Series devices, DH-group 14 is not supported for dynamic VPN.

- On all high-end SRX Series devices, when you enable VPN, overlapping of the IP addresses across virtual routers is supported with the following limitations:

  - An IKE external interface address cannot overlap with any other virtual router.

  - An internal or trust interface address can overlap across any other virtual router.

  - An st0 interface address cannot overlap in route-based VPN in point-to-multipoint tunnels such as NHTB.

  - An st0 interface address can overlap in route-based VPN in point-to-point tunnels.

- On all high-end SRX Series devices, the DF-bit configuration for VPN only works if the original packet size is smaller than the st0 interface MTU, and larger than the **external interface-ipsec overhead**.

- The local IP feature is not supported on the following:

  - All SRX Series devices in chassis cluster configuration

  - All high-end SRX Series devices

- On all high-end SRX Series devices, the IPsec NAT-T tunnel scaling and sustaining issues are as follows:

  - For a given private IP address, the NAT device should translate both 500 and 4500 private ports to the same public IP address.

  - The total number of tunnels from a given public translated IP cannot exceed 1000 tunnels.

Related Documentation

Known Issues

The following problems currently exist in Juniper Networks SRX Series Services Gateways. The identifier following the descriptions is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

NOTE: For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

Application Layer Gateways (ALGs)

- On SRX Series devices, the REAL ALG is not supported, but you can configure it in both CLI and J-Web. PR943123

AppSecure

- In certain cases, configuring AppQoS rules causes the application system cache not to be populated with entries from the application identification results. This might cause performance issues. PR755979

Chassis Cluster

- On all high-end SRX Series devices, in the output of the **show services application-identification application-system-cache** command, the application-system-cache table for P2P encrypted traffic is incorrectly marked as "Encrypted: No" instead of "Encrypted:Yes". PR704023

- On SRX1400 devices in a chassis cluster, after you commit a configuration, the LED changes from green state to off. PR749672

- On SRX5600 and SRX5800 devices in a chassis cluster, when you run the telnet program on either the primary or secondary Routing Engine connecting to SPUs on the Packet Forwarding Engine side, the connection gets stuck because an incorrect source IP is used by the telnet program in the multichassis environment. When the connection gets stuck, specify the local chassis IP by using **-s** parameter as its source IP for the telnet program to connect to SPUs. PR923782

Command-Line Interface (CLI)

- On all high-end SRX Series devices, in the output of the **show services application-identification application-system-cache** command, the application-system-cache table for P2P encrypted traffic is incorrectly marked as "Encrypted: No" instead of "Encrypted:Yes". PR704023

DHCP

- You cannot get the DHCP relay information through SNMP if DHCP relay is configured under the logical system. PR909906

- On all high-end SRX Series devices, after you configure DHCPv6 in IPv6 mode, the dhcpv6 daemon crashes. PR940078

- On all high-end SRX Series devices, DHCPv6 does not work in IPv6 mode. PR942246

Flow and Processing

- When you enable the hardware timestamp, the RPM probes go to the network control queue instead of to the configured forwarding class. PR487948

- When end-to-end debugging is enabled, if the traffic rate is 1000 packets per second (pps) or higher, packet loss is observed. PR786406

- On all high-end SRX Series devices, the XLR ingress paused condition causes traffic drop and latency to the processing traffic. PR829714

- On devices with 1 GB of memory, if the advanced services license is configured with the **reduce-dp-memory** option, memory is not released from the data plane to the control plane.

  As a workaround, when the advanced services license is configured, do not configure the **reduce-dp-memory** option. PR895648

- For SCTP IPv6 traffic in traffic logs, all the source and destination ports are marked as using port 1. PR928916

- When IKE packets are received before Junos OS default applications are pushed to the Packet Forwarding Engine, the IKE sessions will be established without the IKE application having been marked. As a result, the fragmented IKE packet cannot be sent to iked, because the IKE session has not used IKE applications.

As a workaround, clear the old IKE sessions. PR942730

- In next-generation IOCs, when the IPv6 is in packet mode, the screens are not detected. As a workaround, change IPv6 to flow mode.

> NOTE: For IPv6, flow mode is the default mode.

PR944273

General Packet Radio Service (GPRS)

- When both the Gn and Gp interface pass through an SRX Series device, and the Gn interface is NAT-enabled, the restart counter only takes effect on the Gn interface. PR893379

- For GTPv0 and GTPv1, if the time interval between the primary PDP activation message and the secondary PDP activation message is too small, the secondary GTP-U tunnel on the chassis cluster backup node will not be established. Also, "No control tunnel" error counters are detected on the chassis cluster backup node. Because of this error, the secondary GTP-U tunnels creation failure on backup node leads to the failure of the related updating secondary GTP-U tunnels on backup nodes. PR924791 and PR929042

- If the SRX Series device receives delete PDP response messages simultaneously for both secondary and primary PDP, the primary PDP message might be processed first. When the primary PDP tunnels are deleted, all the related secondary PDP tunnels are also deleted. As a result, some of the deleted PDP response messages might drop with "no control tunnel" errors, but all the requested PDP tunnels are deleted and there is no impact on the GTP tunnels. PR929355

Infrastructure

- When all the input parameters for the command **show security match-policies global source-ip <source IP> destination-ip <destination IP> source-port <source port> destination-port <destination port> protocol <protocol>** are not provided, then the management process might be triggered into an infinite loop. This results in high CPU utilization on the Routing Engine. PR893721

Interfaces and Routing

- When you swap the members of a link aggregation group (LAG), a vmcore or a ksyncd core file is generated on the backup Routing Engine. PR711679

- On all high-end SRX Series devices, the loop back CLI configurations **shdsl-options** for "pt" interface are not working as expected. PR798180

- The SHDSL media and statistics counters are not incrementing after the introduction of micro-interruption to the line. The counters are also not cleared even after explicitly using the clear command. PR810334

- If a large number of IPv6 addresses are configured on an interface, or a large number of logical interfaces, on an interface with IPv6 addresses, the kernel might be very busy when the interface is enabled or disabled. Key kernel modules, like TNP/RDP, cannot be scheduled in time under such situations.

  As a workaround, disable **Duplicate Address Detection** on the interface. PR929300

- SFP interfaces ge-0/0/7, ge-0/0/8, and ge-0/0/9 on the 1-Gigabit Ethernet SYSIO card autonegotiate to 10 gigabits per second. PR946581

Intrusion Detection and Prevention (IDP)

- On all high-end SRX Series devices, the All Attacks policy is not supported. The current IDP policy templates supported are dynamic, based on the attack signatures being added. Therefore, the supported templates might eventually grow past the policy size limit. PR876449

Network Address Translation (NAT)

- On devices in a chassis cluster, some persistent NAT table entries cannot be removed on the SPU when the device is under heavy traffic with multiple failovers. PR834823

Screens

- On SRX5400, SRX5600, and SRX5800 Series devices with next-generation SPC cards installed, when IP spoofing is enabled, after you reboot the device under test (DUT), the address books in the Packet Forwarding Engine will be removed and you cannot push them back into the Packet Forwarding Engine . Due to this issue, the IP spoofing does not work after you reboot the DUT.

  As a workaround, to push back the address books, after the device under test (DUT) is online, kill the nsd process from the shell mode or restart nsd from cli using the **restart network-security immediately** command, or disable/enable IP spoofing from the command mode. PR920216

- On SRX5600 devices, when you configure IP spoofing in Layer 2 mode, before defining the IP spoofing and the address books for specific zones, if the **delete security** or **delete security zone/screen/address-book** commands are executed and the configuration is not committed, the addresses in the Packet Forwarding Engine might be incorrect. Due to this issue, the IP spoofing might not work.

  As a workaround, after executing the **delete security** or **delete security zone/screen/address-book** command, commit the configuration before you continue the IP spoofing configuration or if the IP addresses in PFE is not correct, restart nsd from cli using the **restart network-security immediately** command. PR943232

Switching

- When IS-IS is configured between the SRX device and some third-party devices, after the SRX device is rebooted and the IS-IS adjacency is reestablished, the routes advertised by the third-party devices might not install into the routing table in some cases. PR935109

System Logs

- When you reboot the device, cyclic redundancy check (CRC) error logs recorded in chassis log file might appear. However, this does not affect the normal operation of the device and can be ignored. PR877722

- When you upgrade from one release to another, the following error or warning messages are displayed:

  Network security daemon: rtslib: ERROR kernel does not support all messages: expected 102 got 98,a reboot or software upgrade may be required

  Network security daemon: rtslib: WARNING version mismatch for msg unknown: expected 98 got 0,a reboot or software upgrade may be required

  These messages do not affect the unified ISSU. PR926661

- The error **OpenSSL: error:14090086:lib(20):func(144):reason(134)** means that server certificate verification has failed. The certificate might be a self signed certificate or an expired certificate. PR932274

Unified Threat Management (UTM)

- EWF logs are not marked with user role information. PR936799

- On all high-end SRX Series devices, when you install a license, you might see the message **license not valid for this product add license failed**. Even though the message appears, the feature still functions normally. In addition, the **show system license** command does not display the Sophos antivirus, antispam, or Web filtering licenses. PR948347

Virtual Private Networks (VPNs)

- During VPN configuration change with an interface configuration change at the same commit, or after rebooting the device with VPN and interface configured together, the tunnel sessions creation in flowd are missed. This impacts the traffic flow on that tunnel. the invalid bind interface counter returns a nonzero value when you run the **show usp ipsec global-stat** command.

  As a workaround, deactivate IPsec by using the **deactivate security ipsec** command, wait for a few seconds, and then activate IPsec by using the **activate security ipsec** command. For avoiding issue during reboot, please deactivate ipsec configuration first, reboot, and then enable it after reboot. This issue appears for both IPv4 and IPv6 tunnels. PR928945

- When a large number of tunnels are configured and brought up immediately, the IPsec SA might not synchronize from the SPU to the Routing Engine in a scaling environment. PR937201

- On all SRX Series devices with multiple proxy-identity (MPID), the dead routes are seen while moving the st0 interface from one virtual router to another. PR943577

- After traffic-selector configuration is deleted from the VPN configuration object, the data traffic stops passing through the tunnel.

  As a workaround, after deleting the traffic-selector configuration, execute the commit full command instead of commit. PR944598

- When there are more than 100 traffic selectors configured on a VPN configuration object along with configured, established, tunnels, if all IPsec SAs for this VPN configuration object are cleared at the same time (because of a configuration change on a peer or the use of the clear operational command), the bind-interface associated with that VPN configuration object might be marked as down. PR947103

Related Documentation

Resolved Issues

The following are the issues that have been resolved in Junos OS Release 12.1X46-D10 for Juniper Networks SRX Series Services Gateways. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

> **NOTE:** For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

Application Layer Gateways (ALGs)

- The b attribute (pertaining to bandwidth) in a SIP Session Description Protocol (SDP) message was not carried forward after SIP ALG processed the packet. PR875211

- When an RTSP TCP segment cannot be processed because it is too small or incomplete, the RTSP ALG holds it and waits for the next segment. An RTSP endpoint does not receive an ACK for segments that are too small, so it retransmits the segment several times. Eventually, the RTSP endpoint resets the TCP connection. PR887601

- With RTSP ALG traceoption enabled, if failover occurs on the device, it will trigger flowd crash that RTSP ALG receiving interleave RTSP traffic before the RTSP objects are synchronized completely. PR893136

- In rare cases when ALG is used for flow processing MSS (Maximum Segment Size) in TCP 3-way, handshake is announced in one direction with value higher than 32,120, the next packets in opposite direction gets window size value reduced to 0. PR895498

- In certain circumstances, if the OPTIONS method is used to create a call, and the INVITE method is used to reuse the call, the SIP ALG would apply an incorrect state. As a result, the device might drop the ACK of 200-OK. PR898956

- The SCTP module drops the SCCP packet when the received SCCP pointer goes out of order. PR901584

- On devices enabled with the MS-RPC ALG, the flowd process might crash frequently when heavy MS-RPC traffic is processed by the MS RPC ALG. PR907288

AppSecure

- AppID is using order to selectively report nested applications that it has matched in different transactions on the same session. This means that only nested applications with a higher order are reported. The expected behavior is that it should report nested applications as and when it detects them in the transaction. PR914567

Certificate Authority (CA) Profile

- When you run the **show security pki *-certificate** command, the result displays time without a time zone. PR746785

Chassis Cluster

- On devices in a chassis cluster with the second control link connected, when CRM is installed, and the primary node is power-cycled, the primary node takes over RG-0 ownership when the primary node is rebooted. PR679634

- On devices in a chassis cluster, if a reth Layer 3 logical interface is disabled, the reth interface remains active and the direct route for this logical interface is not removed from the forwarding table. All the traffic destined for the disable network still gets routed out to the disabled reth interface. PR740856

- On devices in a chassis cluster, when you execute the **clear system commit** command, it clears commit only from the local node. PR821957

- On devices in a chassis cluster, during a control link failure, if the secondary node is rebooted by control link failure recovery, the rebooted node goes into disabled state even after startup. PR828558

- On SRX1400, SRX3400, and SRX3600 Series devices, under certain conditions, the em0 (tsec1) detection and recovery mechanism is not working as expected. This might cause the chassis cluster to fail, a "split-brain" condition to occur, or all FPCs to be reset on the local node.

  > ℹ️ NOTE: Do not use the security policy count and make sure trace options are disabled. Do not use set security log mode event command; instead use mode stream (default mode).

  PR877604

- On devices in a chassis cluster, the chassisd log outputs are flooded with the following message: **LCC: fru_is_present: out of range slot -1 for SCB**. PR889776

- On devices in a chassis cluster, in certain IPv6 configurations, the SPU sends out packets with an invalid header on the secondary node, which in turn triggers the hardware monitoring failure on the secondary node. PR935874

Command-Line Interface (CLI)

- There is no specific CLI command to display the count of sessions allowed, denied, or terminated because of UAC enforcement. PR733995

- The **show security pki *-certificate** shows the time without a time zone. PR746785

- The output of the **show security pki ca-certificate detail** command includes the Auto-re-enrollment section. This is incorrect because automatic reenrollment is not supported for CA certificates. PR877574

Flow and Processing

- When DNS ALG was enabled, the rewrite rules applied on the egress interface might not work for DNS messages. PR785099

- On all high-end SRX Series devices, when plugins that use TCP proxy (such as ALGs or UTM) are configured, a certain sequence of valid TCP packets crashed the flow daemon (flowd). Repeated crashes of flowd represented an extended denial of service condition for the device. PR791201

- On all high-end SRX Series devices, when fragmented jumbo frames are reassembled in the SPU (reassembling might be required by IDP feature, ALG feature, ESP/AH packets, and L2TP packets) and if the size of the reassembled packet becomes larger than 9712 bytes, the packet is dropped in the internal device, and the device reports XLR egress packets corruption issues. PR819621

- On all high-end SRX Series devices, the SPU level kernel crashed and generated vmcore files when processing traffic that required serialized packet processing in some application modules such as IDP, ALGs, application security, and so on. PR855397

- Current implementation of timeout for http is 1800s, the default timeout should be 300s. PR858621

- Periodic multicast packets such as NTP do not refresh the route, and packets are dropped intermittently. PR869291

- On SRX Series devices, during ARP floods of the data plane Packet Forwarding Engine, the CPU spikes might impact transit and host-bound traffic. PR871704

- On devices in a chassis cluster, after data plane RG1 failover, the RTSP data packet is queued, and a duplicate RTSP data packet is processed by the device; the flowd process crashes and generates core files. PR883397

- When TCP SYN flood protection is enabled and triggered, and if the Window Scaling option is used between a TCP client and server, TCP communication is reset abnormally. PR886204

- On all high-end SRX Series devices, due to incorrect computation of central point IPv6 sessions, the output of the total central point sessions is incorrect for the **show security monitoring fpc number** command. This is only a display issue and does not affect actual central point sessions or the traffic passing through. PR888890

- On SRX1400 devices, the egress packets are dropped. There is an increase in the number of egress packets dropped when the traffic passes through the ports of the SRX1K-SYSIO card. PR899184

- When flow traceoptions are used to debug source NAT traffic, packet filter did not work. This resulted in a large amount of unexpected traces. PR905568

- The CRL download fails for fragmented LDAP packets. PR910947

- On all high-end SRX Series devices, when you delete a large number of interfaces and commit, and immediately add a large number of interfaces and commit, the session scan might fail. The session related to the deleted interface might still be active, in which case the subsequent traffic drops if it matches the old session. This occurs in a scenario when the deleted interface is added back on the "immediately add" action, and the remote host still generates the traffic matching the session. This issue occurs as the session interface is detected in invalid state in flow checking. PR915422

- J-Flow might not work as expected; the cflowd packets are not seen for version 5 and version 8 sampled flows. PR916986

General Packet Radio Service (GPRS)

- If a GTPv1 user plane (GTPv1-U) tunnel update conflicts with a secondary tunnel, then core files are generated. PR888067

- When there is inconsistency in the NAT rule configuration for the IP address in the IP header and in the GTP payload, packets are dropped.

  - When there is a NAT rule for the IP address in the GTP payload and no NAT rule for the IP address in the IP header, the tunnel is set up on a wrong SPU, and the control and data traffic on the tunnel might be dropped.

- When there is a NAT rule for the IP address in the IP header and no NAT rule for the IP address in the GTP payload, the packet is dropped to keep the consistency of the NAT rule configuration.

PR921313

Hardware

- When the device is rebooted, the next-generation SPC card might not boot up due to I2C bus hang. Error messages related to "I2C" errors also appear in the log. PR923255

Infrastructure

- On all high-end SRX Series devices, when the device authentication is through RADIUS server and the password protocol is Microsoft CHAP version 2, the password change operation fails as the user password change is enforced through Microsoft Active Directory server. PR740869

- After an upgrade, you cannot copy files between nodes in a cluster using the **file copy** command. PR817228

- In a DHCP-relay subscriber management environment, with an output firewall filter configured on an IRB interface to discard the DHCP offer packets, while DHCP-relay subscribers log in, the Junos OS kernel tries to free an already freed memory buffer, which causes the kernel to crash and generate core files. PR824470

- When the backup Routing Engine kernel fails, some devices send a message to the master Routing Engine to generate a core file. PR854501

- On SRX1400 devices with 10-Gigabit Ethernet, when the system I/O card is inserted on SFP-T of ge-0/0/7, ge-0/0/8, or ge-0/0/9 interface, the device interface LEDs light immediately. PR865899

- If the secondary control link (em1) interface uses SFP-T, the interface is down when you add node 1 to the cluster. PR873253

- On devices in a chassis cluster, after control plane Redundancy Group (RG0) failover, SPUs might have more if states than the new master Routing Engine. This difference leads to sequence number mismatch and causes cold synchronization failure, and all FPCs might reboot. After the FPCs reboot, a "split brain" situation occurs in which both nodes become primary. PR885889

- E2edebug traces are not generated for all the events. PR919471

Interfaces and Routing

- On the K2-Routing Engine (64-bit Routing Engine) when speed or link mode are statically configured on the device for the fxp0 interface, the driver for fxp0 accepts the configuration from DCD process. The K2-Routing Engine does not propagate the setting to the hardware driver. Instead, the driver setting is forced to auto-negotiate. Thus, as the fxp0 interface is auto-negotiating, and the far end device is forced to 100/full, the auto-negotiation on fxp0 will detect the speed but will not detect the duplex and hence, defaults that duplex to half-duplex. PR704740

- On VLAN tagged Ethernet frames (802.1p), you cannot modify the VDSL priority bits. PR817939

- Multicast stream is redirected to other member links on the ae interface or on the reth LAG even when the link in use is disabled. PR867529

- When a SHDSL Mini-PIM is configured in 2-wire mode with annex mode as Annex B/G, one of the physical interfaces does not come up. PR874249, PR882035

- On devices in a chassis cluster, when a session created as the incoming interface is a VPN secure tunnel interface (ST interface) and the outgoing interface is a logical tunnel interface (LT interface), this session is incorrectly marked as active on the secondary node. When this session expires on the secondary node, the sessions on both cluster nodes might get deleted and interrupt the traffic. PR896299

- When multiple routing instances are defined, DNS names in the address-book entries might not get resolved. This results in corresponding security policies to be nonoperational. PR919810

- When multiple IP addresses from an overlapping subnet are configured on a single interface, the interface enable-related or disable-related changes might not work. PR920993

Intrusion Detection and Prevention (IDP)

- On XLP platforms, setting the **max-sessions** option in an application identification configuration did not impact the attack traffic. PR809384

- After the Junos image is upgraded, we recommend that you download a completely updated IDP security package and then perform the installation. Subsequent incremental updates (default) work fine. If a complete update is not performed, the device might end up adding only the new signatures downloaded in incremental order, leaving the device unprotected from a large set of signatures. PR876764

- On SRX Series devices with IDP enabled, if IDP exempt rule is configured, a change of the IDP rule configuration (such as a change to source or destination, action, or signature) might cause the flowd process to crash and core files are generated. PR877865

- When there are a large number of ASC entries (100,000 or more), and the entries are listed using CLI command, the flowd process might crash. PR886173

- On all high-end SRX Series devices, maximize sessions inline-tap equal mode is not supported in Junos OS Release 12.1X46-D10. If the maximize sessions inline-tap equal

mode is configured in a release earlier than Junos OS Release 12.1X46-D10, when you upgrade to Junos OS Release 12.1X46-D10, the configuration changes to maximize sessions inline-tap firewall mode. PR889597

- On SRX Series devices, the flowd process might crash when IDP is enabled using software based pattern matching and detects more than one attack entry for the same attack. PR907703

J-Web

- The J-Web interface was vulnerable to HTML cross-site scripting attacks, also called XST or cross-site tracing. PR752398

- In J-Web, SRX Series devices fail to downgrade from Junos OS Release 12.1X46-D10 through HTTP file upload. PR918112

- In J-Web, if the policy name was "0", the penultimate-hop popping (PHP) function treated it as empty, and traffic log output could not be viewed. PR853093

- In J-Web, the LSYS operation might cause MGD to generate a core file, and **compare before commit** does not work. PR889029

Network Address Translation (NAT)

- Under certain conditions, a duplicate SNMP index might be assigned to different interfaces by the kernel to the mib2d (Management Information Base II daemon). This might cause mib2d and other processes such as lacpd (LACP daemon) to crash and generate core files. PR836823

- On devices enabled with the PIM protocol, the flowd process crashed and generated core files, when there was a unicast PIM register message received with encapsulated multicast data; and if NAT process was involved in the session for the received PIM packet. This issue was observed on standalone high-end SRX Series devices, and on devices in a chassis cluster. In the case of devices in a chassis cluster, the flowd process crashed on both node 0 and node 1. PR842253

- In a root system, the destination and static NAT rule cannot send system log and trap messages when the number of sessions reaches the threshold value. In a logical-system, the source, destination, and static NAT rule cannot send system log and trap messages when the number of sessions reaches the threshold value. PR905359

- On devices in a chassis cluster, the chassis cluster rule number of sessions in the SNMP query or walk result is the sum of the real number of sessions of the primary node and the secondary node. PR908206

- On all high-end SRX Series devices, when source NAT is configured with persistent NAT enabled, sometimes the persistent NAT bindings leak on the central point. PR910116

Routing Policy and Firewall Filters

- If more than 10 virtual routers (routing instances) or logical systems (LSYS) are configured on a device, DNS fails to resolve addresses. A maximum of only 10 routing instances and LSYS can be configured per DNS name server. PR896174

Screen

- On all high-end SRX Series devices with IP spoofing screen enabled, the routing table search fails when it is locked by the system. As a result, false positives occur on IP spoofing detection. PR901507

- On all high-end SRX Series devices, security screen are not allocated for more than 165 zones due to memory limitation. If a security screen is enabled for more than 165 zones, only 165 zones are actually enabled and the memory is exhausted by the screen allocation, resulting in traffic interruption. PR913052

System Log

- On SRX3400 and SRX3600 devices, the following system logs are seen in the messages file:

  sfchip_show_rates_pfe: Fchip Plane 0, dpc 0, pfe <1/2/3>: Invalid dpc

  These system logs do not affect the device. PR738199

- Fetching ppX interface statistics leaks in pfestat_table leads to the following error logs:

  pfestat_req_add: pfestat table out of ids

  During this state it is not possible to fetch any interface statistics. PR751366

- On all high-end SRX Series devices, when a Routing Engine card is removed and placed again, swapped, or rebooted, the following error message appears in the system log for an hour:

  No response from the other routing engine for the last 300 seconds

  PR875189

- SRX5600 and SRX5800 devices with an SRX5K-SPC-4-15-320 (next-generation SPC) might generate one of the following system logs on the messages file:

  spu_mac_get_linkstate:spu (<fpc#>/<pic#>) – phy link<link#> failed

  spu_mac_get_linkstate:%PFE-3:(<fpc#>/<pic#>) –MAC layer link failed

  In this condition, the affected SPU cannot do any flow processing until the system is rebooted. PR914736

- On SRX1400 devices in some cases, the traffic gets interrupted for about 5 seconds occasionally and the following log message appears:

  XLR ingress pause

PR921692

- The session ID of AppTrack logs does not include the SPU ID. Hence, there is a mismatch with firewall log session ID and AppTrack log session ID of the same session. The AppTrack log now has the same session id used in the firewall logs.PR924941

Unified Threat Management (UTM)

- The enhanced Web filter parser mishandles the URL and host from the HTTP header. This results in an "uncategorized" EWF reply. PR862602

Virtual Private Networks (VPNs)

- On a SRX Series device, when a session is closed because the user for that session has signed out from the Junos Pulse, the session close log shows the role information as "N/A". PR689607

- An IPsec policy for a VPN can contain proposals with different protocol types (ESP or AH). This means that an IPsec SA can be established with either ESP or AH, depending on the protocol type of the peer's proposal. PR843281

- When IPsec VPN Internet Key Exchange (IKE) traffic passed through the device, memory leaks were observed and the VPN connection could not be established. PR857013

- On all high-end SRX Series devices, the Junos Pulse client has been updated from Release 2.0R3 to 4.0R2. PR868101

- File Descriptor leak occurs during the network-security-trace process when commit configuration changes are made in the **edit security ike** configuration. Eventually, the system reaches the maximum file limit, which results in a system-unmanageable condition. PR893017

- In a site-to-site IPsec VPN deployments using IKEv2, when tunnels are removed through configuration change, the information is not propagated to the remote peer. Later, when the peer initiates a normal Phase-1 re-key process, the kmd process crashes and core files are generated. PR898198

Related Documentation

Documentation Updates

This section lists the errata and changes in Junos OS Release 12.1X46-D10 documentation.

Documentation Updates for the Junos OS Software Documentation

This section lists improvements and outstanding issues with the software documentation.

Junos OS for SRX Series Documentation

The Junos OS for SRX Series technical documentation set has been expanded, restructured, and retitled in Junos OS Release 12.1X46-D10 to make it more comprehensive, easy-to-use, and intuitive. Highlights:

- (New) The Complete Software Guide consolidates all of the release-specific content that applies to Junos OS for SRX Series devices (except release notes) into a three volume set of PDFs that you can download and view offline. The first volume contains getting started and administration information; the second contains feature information; the third contains developer information. You can find the PDFs in the Downloads box on the right side of the *Junos OS for SRX Series Services Gateways, Release 12.1X46* index page.

- (New) The *Getting Started Guide for Branch SRX Series* describes how to get up and running with branch SRX Series devices.

- (Expanded) The *Junos OS Monitoring and Troubleshooting Library for Security Devices* contains significantly more content to help network and security managers keep their SRX Series devices running smoothly in their production environments.

- (Expanded) The *Junos OS for SRX Series Services Gateways, Release 12.1X46* index page has been expanded to serve as a "one stop shop" for all of your Junos OS for SRX Series technical documentation needs.

BGP Feature Guide for Security Devices

- In "Example: Configuring Route Authentication for BGP," the following configuration steps in the CLI quick configuration and in the step-by-step procedure sections are not supported on SRX Series devices:

```
set security authentication-key-chains key-chain bgp-auth tolerance 30
set security authentication-key-chains key-chain bgp-auth key 0 secret
this-is-the-secret-password
set security authentication-key-chains key-chain bgp-auth key 0 start-time
2011-6-23.20:19:33-0700
set security authentication-key-chains key-chain bgp-auth key 1 secret
this-is-another-secret-password
set security authentication-key-chains key-chain bgp-auth key 1 start-time
2012-6-23.20:19:33-0700
```

J-Web

- **J-Web pages for stateless firewall filters**—There is no documentation describing the J-Web pages for stateless firewall filters. To find these pages in J-Web, go to **Configure>Security>Firewall Filters**, and then select **IPv4 Firewall Filters** or **IPv6 Firewall Filters**. After configuring the filters, select **Assign to Interfaces** to assign your configured filters to interfaces.

SNMP MIBs and Traps Reference

- The "Enterprise-Specific MIBs and Supported Devices" topic incorrectly states that the SNMP IDP MIB is supported on high-end SRX Series devices. The SNMP IDP MIB is not supported on high-end SRX Series devices.

Modem Interfaces Feature Guide for Security Devices

- The Example: Configuring the 3G Wireless Modem Interface in Modem Interfaces Guide provides the following incorrect information for configuring a dialer filter for the 3G wireless modem interface:

  - user@host# **set firewall family inet dialer-filter corporate-traffic-only term term1 from source-address 20.20.90.4/32**

  - user@host# **set firewall family inet dialer-filter corporate-traffic-only term term1 from destination-address 200.200.201.1/32**

  - user@host# **set firewall family inet dialer-filter corporate-traffic-only term term1 then note**

  The following incorrect configuration output is included:

  ```
      [edit]
  user@host# show firewall family inet dialer-filter corporate-traffic-only
  term term1 {
    from {
      source-address {
        20.20.90.4/32;
      }
      destination-address {
        200.200.201.1/32;
      }
    }
    then note;
  }
  ```

  The correct configuration is:

  user@host# **set firewall family inet dialer-filter corporate-traffic-only term term1 then note**

  The following configuration is output from the correct configuration:

  ```
      [edit]
  user@host# show firewall
  family inet {
  ```

```
        dialer-filter corporate-traffic-only {
          term term-1 {
            then note;
          }
        }
      }
```

Network Address Translation

The command **show security nat source persistent-nat-table** under **Network Address Translation > Administration > Source NAT Operational Commands** has the following errors:

- The command is missing the **summary** option:**summary**—Display persistent NAT bindings summary.

- The command contains incomplete sample output —The corrected sample output is as follows:

show security nat source persistent—nat—table internal-ip internal-port

```
user@host> show security nat source persistent—nat—table internal-ip 9.9.9.1 internal-port 60784


Internal                        Reflective        Source      Type
Left_time/  Curr_Sess_Num/ Source
 In_IP  In_Port I_Proto Ref_IP    Ref_Port R_Proto NAT Pool
Conf_time   Max_Sess_Num  NAT Rule
9.9.9.1  60784   udp  66.66.66.68  60784     udp   dynamic-customer-source
any-remote-host  254/300  0/30 105
```

show security nat source persistent—nat—table all

```
user@host> show security nat source persistent—nat—table all
 Internal            Reflective                Source      Type
Left_time/  Curr_Sess_Num/  Source
 In_IP     In_Port I_Proto Ref_IP       Ref_Port R_Proto NAT Pool
     Conf_time   Max_Sess_Num    NAT Rule
9.9.9.1    63893    tcp    66.66.66.68    63893    tcp    dynamic-customer-source
 any-remote-host  192/300    0/30 105
9.9.9.1    64014    udp    66.66.66.68    64014    udp    dynamic-customer-source
 any-remote-host  244/300    0/30 105
9.9.9.1    60784    udp    66.66.66.68    60784    udp    dynamic-customer-source
 any-remote-host  254/300    0/30 105
9.9.9.1    57022    udp    66.66.66.68    57022    udp    dynamic-customer-source
 any-remote-host  264/300    0/30 105
9.9.9.1    53009    udp    66.66.66.68    53009    udp    dynamic-customer-source
 any-remote-host  268/300    0/30 105
9.9.9.1    49225    udp    66.66.66.68    49225    udp    dynamic-customer-source
 any-remote-host  272/300    0/30 105
9.9.9.1    52150    udp    66.66.66.68    52150    udp    dynamic-customer-source
 any-remote-host  274/300    0/30 105
9.9.9.1    59770    udp    66.66.66.68    59770    udp    dynamic-customer-source
 any-remote-host  278/300    0/30 105
9.9.9.1    61497    udp    66.66.66.68    61497    udp    dynamic-customer-source
 any-remote-host  282/300    0/30 105
9.9.9.1    56843    udp    66.66.66.68    56843    udp    dynamic-customer-source
 any-remote-host   -/300    1/30 105
```

show security nat source persistent-nat-table summary

```
user@host> show security nat source persistent-nat-table summary
Persistent NAT Table Statistics on FPC5 PIC0:
binding total : 65536
binding in use : 0
enode total : 524288
enode in use : 0
```

Routing Protocols Overview for Security Devices

- The default route preference value in the "Understanding Route Preference Values" topic for Static and Static LSPs lists the values incorrectly. The correct values are as follows:

How Route Is Learned	Default Preference
Static	5
Static LSPs	6

Security Policy Applications Feature Guide for Security Devices

- On the Overview tab, under IP-Related Predefined Policy Applications, in the topic entitled "Understanding IP-Related Predefined Policy Applications," the Port column for both TCP-ANY and UDP-ANY should indicate 0-65535. The lead-in sentence should read, "Each entry includes the port and a description of the application." TCP-ANY means any application that is using TCP, so there is no default port for it. The same is true for UDP-ANY.

- In the topic entitled "Understanding Miscellaneous Predefined Policy Applications," table "Predefined Miscellaneous Applications" is incomplete. Under the RADIUS row, add a new row:

Table 12: Predefined Miscellaneous Applications

Application	Port	Description
RADIUS Accounting	1813	Enables the collecting of statistical data about users logging in to or out from a LAN and sending the data to a RADIUS Accounting server.

In table "Predefined Miscellaneous Applications" replace the IPsec-NAT row with the following:

Table 13: Predefined Miscellaneous Applications

Application	Port	Description
IKE	500	Internet Key Exchange is the protocol that sets up a security association in the IPsec protocol suite.
IKE-NAT	4500	Helps to perform Layer 3 NAT for S2C IKE traffic.

Table 14: Predefined Miscellaneous Applications

Application	Port	Description
VoIP	389	Internet Locator Service (ILS)
	522	User Location Service (ULS)
	1503	T.120 Data sharing
	1719	H.225 RAS message
	1720	Q.931 Call Setup
	1731	Audio Call Control
	5060	SIP protocol

Various Guides

- Some Junos OS user, reference, and configuration guides—for example the Junos Software Routing Protocols Configuration Guide, Junos OS CLI User Guide, and Junos OS System Basics Configuration Guide—mistakenly do not indicate SRX Series device support in the "Supported Platforms" list and other related support information; however, many of those documented Junos OS features are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, please refer to Feature Explorer:
  http://pathfinder.juniper.net/feature-explorer/select-software.html?swName=Junos+OS&typ=1.

Documentation Updates for the Junos OS Hardware Documentation

This section lists outstanding issues with the hardware documentation.

SRX5600 Services Gateway Hardware Guide

- The "Accessory Box Parts List" table in the "Verifying the SRX5600 Services Gateway Parts Received" topic lists the quantities for split washers, DC power terminal lugs, and 3 in. x 5 in. pink bag incorrectly. The correct quantities are as follows:

Part	Quantity
Split washers 1/4	34
DC power terminal lugs, 6-AWG	9
3 in. x 5 in. pink bag	5

The "Accessory Box Parts List" table in the "Verifying the SRX5600 Services Gateway Parts Received" topic is missing the following information:

Part	Quantity
Screws (4 x 8 mm long, 1.5 mm pitch)	4
SFP, Gigabit Ethernet, 850 nm, 550 m reach, SX, DDM	2
Fiber optic cable, Duplex, LC/LC, Multimode, 3 m	1

Related Documentation

- New and Changed Features on page 78
- Known Behavior on page 102
- Known Issues on page 121
- Resolved Issues on page 126

Migration, Upgrade, and Downgrade Instructions

This section includes the following topics:

- Upgrading and Downgrading among Junos OS Releases on page 140
- Upgrading an AppSecure Device on page 142
- Network and Security Manager Support on page 142
- Upgrade and Downgrade Scripts for Address Book Configuration on page 143
- Upgrade Policy for Junos OS Extended End-Of-Life Releases on page 145
- Hardware Requirements on page 145

Upgrading and Downgrading among Junos OS Releases

All Junos OS releases are listed in sequence on the JUNOS Software Dates & Milestones webpage:

http://www.juniper.net/support/eol/junos.html

To help in understanding the examples that are presented in this section, a portion of that table is replicated here. Note that releases footnoted with a 1 are Extended End-of-Life (EEOL) releases.

Product	FRS Date
Junos 12.1	03/28/2012
Junos 11.4[1]	12/21/2011
Junos 11.3	08/15/2011
Junos 11.2	08/03/2011
Junos 11.1	03/29/2011
Junos 10.4[1]	12/08/2010
Junos 10.3	08/15/2010
Junos 10.2	05/28/2010
Junos 10.1	02/15/2010
Junos 10.0[1]	11/04/2009
Junos 9.6	08/06/2009
Junos 9.5	04/14/2009
Junos 9.4	02/11/2009
Junos 9.3[1]	11/14/2008
Junos 9.2	08/12/2008
Junos 9.1	04/28/2008
Junos 9.0	02/15/2008
Junos 8.5[1]	11/16/2007

You can directly upgrade or downgrade between any two Junos OS releases that are within three releases of each other.

- Example: Direct release upgrade

  Release 10.3 → *(bypassing Releases 10.4 and 11.1)* Release 11.2

To upgrade or downgrade between Junos OS releases that are more than three releases apart, you can upgrade or downgrade first to an intermediate release that is within three releases of the desired release, and then upgrade or downgrade from that release to the desired release.

- Example: Multistep release downgrade

  Release 11.3 → *(bypassing Releases 11.2 and 11.1)* Release 10.4 → Release 10.3

Juniper Networks has also provided an even more efficient method of upgrading and downgrading using the Junos OS EEOL releases. EEOL releases generally occur once a calendar year and can be more than three releases apart. For a list of, EEOL releases, go to http://www.juniper.net/support/eol/junos.html

You can directly upgrade or downgrade between any two Junos OS EEOL releases that are within three EEOL releases of each other.

- Example: Direct EEOL release upgrade

  Release 9.3 (EEOL) → *(bypassing Releases 10.0 [EEOL] and 10.4 [EEOL])* Release 11.4 (EEOL)

To upgrade or downgrade between Junos OS EEOL releases that are more than three EEOL releases apart, you can upgrade first to an intermediate EEOL release that is within three EEOL releases of the desired EEOL release, and then upgrade from that EEOL release to the desired EEOL release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 8.5 (EEOL) → *(bypassing Releases 9.3 [EEOL] and 10.0 [EEOL])* Release 10.4 (EEOL) → Release 11.4 (EEOL)

You can even use a Junos OS EEOL release as an intermediate upgrade or downgrade step if your desired release is several releases later than your current release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 9.6 → Release 10.0 (EEOL) → Release 10.2

For additional information about how to upgrade and downgrade, see the *Junos OS Installation and Upgrade Guide*.

Upgrading an AppSecure Device

Use the no-validate Option for AppSecure Devices.

For devices implementing AppSecure services, use the no-validate option when upgrading from Junos OS Release 11.2 or earlier to Junos OS 11.4R1 or later. The application signature package used with AppSecure services in previous releases has been moved from the configuration file to a signature database. This change in location can trigger an error during the validation step and interrupt the Junos OS upgrade. The no-validate option bypasses this step.

Network and Security Manager Support

Network and Security Manager (NSM) support for High-End SRX Series Services Gateways with Junos OS 12.1X46-D10 is available only with NSM versions 2012.2R6 / 2012.1R10 and later. For additional information, see Network and Security Manager documentation.

Upgrade and Downgrade Scripts for Address Book Configuration

Beginning with Junos OS Release 11.4 or later, you can configure address books under the [security] hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the [security zones] hierarchy (zone-defined configuration).

You can either define all address books under the [security] hierarchy in a zone-attached configuration format or under the [security zones] hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see Figure 7 on page 144).

- About Upgrade and Downgrade Scripts on page 143
- Running Upgrade and Downgrade Scripts on page 144

About Upgrade and Downgrade Scripts

After downloading Junos OS Release 12.1, you have the following options for configuring the address book feature:

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

- **Use the upgrade script**—You can run the upgrade script available on the Juniper Networks support site to configure address books using the new zone-attached configuration format. When upgrading, the system uses the zone names to create address books. For example, addresses in the trust zone are created in an address book named **trust-address-book** and are attached to the trust zone. IP prefixes used in NAT rules remain unaffected.

  After upgrading to the zone-attached address book configuration:

  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.

  - You cannot configure address books using the J-Web interface.

  For information on how to configure zone-attached address books, see the Junos OS Release 11.4 documentation.

- **Use the downgrade script**—After upgrading to the zone-attached configuration, if you want to revert to the zone-defined configuration, use the downgrade script available on the Juniper Networks support site. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

> NOTE: Before running the downgrade script, make sure to revert any configuration that uses addresses from the global address book.

Figure 7: Upgrade and Downgrade Scripts for Address Books
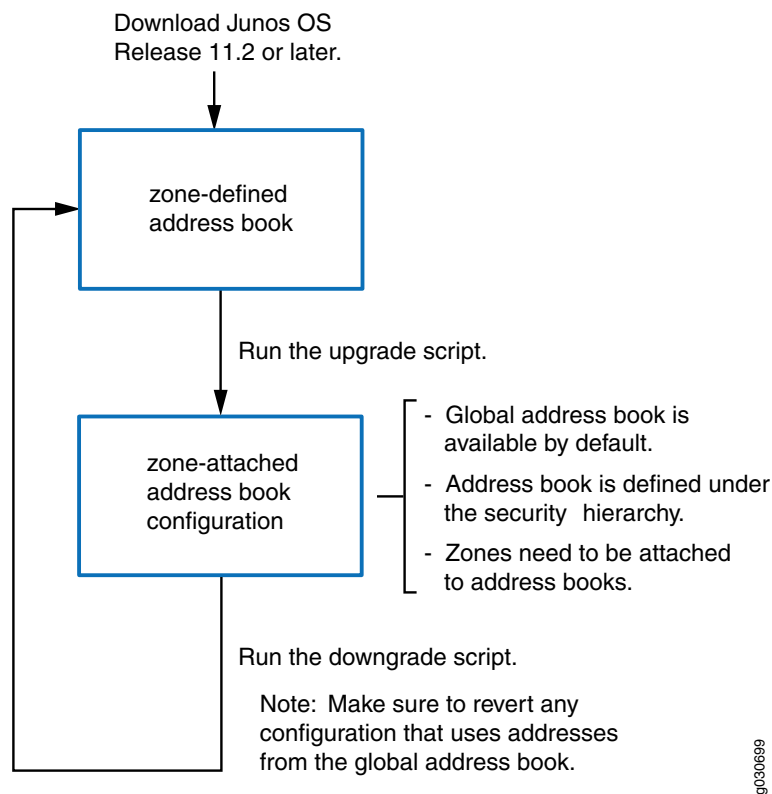
Running Upgrade and Downgrade Scripts

The following restrictions apply to the address book upgrade and downgrade scripts:

- The scripts cannot run unless the configuration on your system has been committed. Thus, if the zone-defined address book and zone-attached address book configurations are present on your system at the same time, the scripts will not run.

- The scripts cannot run when the global address book exists on your system.

- If you upgrade your device to Junos OS Release 11.4 or later and configure logical systems, the master logical system retains any previously configured zone-defined address book configuration. The master administrator can run the address book upgrade script to convert the existing zone-defined configuration to the zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems.

> NOTE: You cannot run the downgrade script on logical systems.

For information about implementing and executing Junos operation scripts, see the *Junos OS Configuration and Operations Automation Guide*.

Upgrade Policy for Junos OS Extended End-Of-Life Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information on EEOL releases and to review a list of EEOL releases, see http://www.juniper.net/support/eol/junos.html .

Hardware Requirements

Transceiver Compatibility for SRX Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on high-end SRX Series Services Gateways interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport SFP interface modules as long as they are provided by Juniper Networks. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

Related
Documentation

Product Compatibility

-

Hardware Compatibility

To obtain information about the components that are supported on the device, and special compatibility guidelines with the release, see the SRX Series Hardware Guide.

To determine the features supported on SRX Series devices in Junos OS Release 12.1X46-D10, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at:

http://pathfinder.juniper.net/feature-explorer/.

Third-Party Components

This product includes third-party components. To obtain a complete list of third-party components, see Copyright and Trademark Information.

Finding More Information

For the latest, most complete information about known and resolved issues with the Junos OS, see the Juniper Networks Problem Report Search application at:

http://prsearch.juniper.net.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at:

http://pathfinder.juniper.net/feature-explorer/.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at:

http://www.juniper.net/techpubs/content-applications/content-explorer/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number

- Page number

- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.

- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.

- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/

- Search for known bugs: http://www2.juniper.net/kb/

- Find product documentation: http://www.juniper.net/techpubs/

- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/

- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/

- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/

- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at https://tools.juniper.net/SerialNumberEntitlementSearch/.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .

- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

`user@host>` **request support information** | **save** *filename*

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to **support@juniper.net**. For documentation issues, fill out the bug report form located at https://www.juniper.net/cgi-bin/docbugreport/.

Revision History

19 December 2013—Revision 1, Junos OS 12.1X46-D10 – High-End SRX Series, Branch SRX Series, and J Series.